•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Internal Audit Report

Fraud and Serious Organised Crime

26 September 2022 (management actions agreed November 2023 following phased implementation)

CW2009

Overall Assessment	**Limited Assurance**

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings have been raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Significant improvement required

Overall opinion and summary of findings

Significant control weaknesses were identified in both the design and effectiveness of the Council's fraud and serious organised crime (SOC) (including anti-money laundering (AML)) control environment and governance and risk management frameworks.

Consequently, only limited assurance can be provided that fraud and SOC risks are being identified and effectively managed, and that the Council's objectives of managing and mitigating the impacts of fraud and serious organised crime will be achieved.

Ongoing Assurance

Review of a sample of established first line service fraud management arrangements confirmed that (whilst inconsistent) they were generally well designed, although there is currently no ongoing service and directorate (first line) or established second line assurance performed to confirm their ongoing effectiveness.

A lack of ongoing assurance presents a challenge for individual directors and the Corporate Leadership Team (CLT) in meeting their responsibilities outlined in Council policies to ensure that the Council develops and maintains effective controls to detect and prevent fraud, bribery, and anti-money laundering.

The Council also has limited assurance that new controls are being designed and implemented to combat the pace and consistently changing nature of fraudulent activity.

It is acknowledged that this may be addressed by implementation of the planned governance and assurance model, and that external audit will provide some assurance on key financial controls during to support preparation of the financial statements.

Reporting

There is no established Council-wide process for recording fraud; SOC; and AML incidents, across Council services, or consolidated reporting provided to directorates and the CLT to provide a view on the volume; nature; and impact of frauds that occur. Consequently, the Council has no overarching view of the volume and impact (including the financial impact) of incidents and cannot clearly define whether and what action is required to improve the design and effectiveness of established fraud prevention and detection controls.

Whilst there is a clearly defined escalation route for fraud and SOC incidents defined in Council policies to the Chief Executive; Monitoring Officer; Money Laundering Reporting Officer; and Chief Internal Auditor; numbers reported are low.

This suggests either the volume; nature; and impact of fraud experienced across the Council is immaterial, or that fraudulent activity is potentially not being identified and escalated in line with established policy requirements.

Risk Management

Fraud and SOC is an enterprise risk for the Council, which is reviewed and assessed regularly at a Council wide level, however there is no established process in place to identify and manage thematic service fraud and SOC risks across the Council.

The Corporate Resilience team were advised through previous discussions with the Corporate Risk Team circa 2019, that consideration of fraud and SOC related risks should be performed within individual service areas as part of the Council's corporate risk management approach.

Phased Implementation Approach

A phased implementation approach will be adopted, to enable sufficient time for the design and implementation of the new process. The new process should give consideration to Audit Scotland expectations as detailed in their July 2022 publication on Fraud and Irregularity.

Following review of arrangements during 2023 by the Council's Fraud and SOC working group, management actions were agreed in November 2023.

Audit Assessment

Audit Areas	Findings	Priority Rating		Areas of good practice
1. Anti-Money Laundering Arrangements 2. Strategy and Governance 3. Training 4. Partnering 5. First line arrangements	1. Established Fraud and Serious Organised Crime Arrangements	**High Priority**		• Fraud prevention, Anti-bribery, and Anti-Money Laundering policies have been established and are published on the Council's intranet (the Orb). • The Council has established a Serious Organised Crime Group which includes a wide breadth of representation across the Council with external input (such as Police Scotland) as required. • The Council has a clearly defined risk appetite for fraud and SOC. • An annual fraud and detection report provides details on fraud detection and prevention activities undertaken by the Customer Fraud Team and outcomes of the NFI exercise. • Information sharing protocols in relation to Fraud and SOC are in place. • The Council participates in the Scottish Local Authority Investigators Group (SLAIG) and the Institute of Revenues Rating and Valuations (IRRV) professional group. • The services most likely to be impacted by fraud and SOC have established fraud prevention and detection processes. • There is a clearly defined fraud and SOC escalation route to the Council's Monitoring Officer; Chief Internal Auditor; and Chief Executive; and a clearly defined escalation rout to the Money Laundering Reporting Officer (MLRO), together with a requirement for provision of an annual money laundering report by the MLRO to the Governance, Risk, and Best Value Committee. • The Council's external website includes a link to an electronic fraud form enabling citizens and other parties to report a possible fraud. • Various training and awareness sessions for employees and elected members have been facilitated by the Corporate Resilience team.
	2. Risk Management – Fraud and SOC	**Medium Priority**		

Background and Scope

The Scottish Government's Serious Organised Crime Strategy outlines how Scotland should work together to reduce the harm caused by serious organised crime (SOC). The Strategy defines SOC as a crime that:

- involves more than one person
- is organised, involving a level of control, planning and specialist resources
- causes, or has the potential to cause, significant harm
- involves financial or other benefit to the individuals concerned

Local authorities (LAs) face significant risks related to fraudulent transactions and other criminal activities, including money laundering, perpetrated by SOC groups. Further areas of risk and vulnerability related to serious and organised crime include cybercrime, human trafficking, bogus tradespeople, inadvertent funding of SOC groups through procurement and licensing activities, counterfeit goods etc.

LAs can be used by criminals and anti-social elements to facilitate their money laundering activities.

Relevant Legislation and Guidance

Relevant fraud, Anti-Money Laundering (AML), and SOC legislation that applies to the Council includes:

- Criminal Justice and Licensing (Scotland) Act 2010
- Serious Crime Act 2007
- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017

Whilst LAs are not directly included within the scope of anti-money laundering legislation, the Chartered Institute of Public Finance and Accountancy (CIPFA) advises LAs to proactively comply with the underlying principles of the anti-money laundering legislation and regulations, and not to presume that money laundering isn't an issue for local government.

Consequently, CIPFA considers that it is good practice for LAs to appoint a designated Money Laundering Reporting Officer (MLRO) and apply AML policies and procedures.

LAs are also expected to play active part in the wider remit of the Scottish Government Serious Organised Crime Strategy through active cooperation with the wider network of partnering agencies, including provision of good quality data for the purpose of knowledge sharing / data matching exercises.

Covid-19 Impacts

Recent CIPFA and Audit Scotland publications have highlighted significantly increased fraud and SOC risks, as a result of the Covid-19 pandemic. These are primarily due to high amounts of funding distributed by public bodies; the need to respond quickly; relaxation of certain public contract procurement and grant approval requirements; and the impact of homeworking and physical distancing on routine validation and data security checks.

The Council's approach to Fraud and SOC

Key Council policies designed to ensure compliance with applicable legislation and manage the Council's potential fraud and SOC risks include:

- Fraud Prevention Policy
- Anti-Bribery Policy
- Whistleblowing Policy
- Employee Code of Conduct

The Council's Fraud and SOC Framework

The Council has no established second line framework that provides fraud and SOC guidance to directorates and services, and no centralised reporting and oversight of fraud and SOC incidents.

Each directorate and their services are responsible for identifying their relevant fraud and SOC risks and implementing appropriate processes; procedures; and controls to ensure that these risks are effectively managed and confirm alignment with the Council policies noted above. This will often involve working closely with multi agency partners (for example Police Scotland).

It is acknowledged that implementation of a framework would be complex given the volume and variation of fraud and SOC risks that could potentially impact a number of Council services, and the complex governance and oversight of these services and their associated risks performed by relevant executive committees.

Council Serious Organised Crime Group

The Council's SOC Group was established at the request of the Corporate Leadership Team (CLT) to coordinate and monitor the Council's fraud and SOC activities in response to Scotland's SOC Strategy. The Group is chaired by the Resilience Manager, who has delegated responsibility for the coordination of the Council's response to serious and organised crime including:

- raise awareness of potential vulnerability from SOC and other forms of corrupt practice
- enhance resilience against corrupt practice
- develop, agree and monitor the annual workplan
- share good practice
- ensure appropriate infrastructures and internal controls are in place

corporately promote the benefits of positive ethics and integrity.

The Council's SOC group meets quarterly and reports to the Edinburgh Multi-Agency Serious Organised Crime Board chaired by Police Scotland.

The Council's SOC group is also responsible for completion of the Local Authority Serious and Organised Crime Checklist provided by SOLACE. The checklist is designed to be used as an internal self-assessment tool by senior management to provide a high-level overview of the serious and organised crime risks that could potentially impact each authority.

Customer Fraud Team (CFT) and National Fraud Initiative

The Council's CFT investigates and recovers the proceeds from fraudulent activity reported by members of the public or other government agencies. This includes external fraud home visits.

The Council also participates in Audit Scotland's National Fraud Initiative (NFI) exercise, which is a comprehensive data matching exercise completed over a two-year period that compares information held by public bodies to highlight discrepancies between the records held across various public organisations and identify any potential instances of fraud.

An annual fraud and detection report is presented to the Finance and Resources Committee which provides details on fraud detection and prevention activities undertaken by the Customer Fraud Team and outcomes of the NFI exercise.

Scope

This review assessed the adequacy of the design of the governance arrangements and operational processes and controls established by directorates to support services with effective management of their fraud and serious organised crime risks, and established assurance arrangements to confirm that processes and controls are being consistently and effectively applied.

We also considered the processes established to support completion of the UK Government's local authority serious and organised crime checklist, and the adequacy and effectiveness of governance arrangements established to provide a holistic view of the management of fraud and SOC risks and incidents across the Council, with focus on the areas detailed below:

- Licensing
- Planning and Development Management
- Council housing allocations and end of tenancy agreements
- Finance and Procurement
- Customer and Digital Services (CFT and financial transaction processing)

Alignment to CLT Risks

- Fraud and Serious Organised Crime

Limitations of Scope

This review was limited to assessing the design of the Council’s established fraud and SOC governance and risk management processes and supporting policies; procedures; and controls but did not consider their effectiveness.

Whistleblowing was also specifically excluded from the scope of this review as this was considered by the separate independent review.

Reporting Date

Testing considered the period 2017 to 2022. Audit work concluded on 20 September 2022, and findings and opinion are based on the conclusion of work as at that date

Following review of arrangements during 2023 by the Council’s Fraud and SOC working group, management actions were agreed in November 2023.

Findings and Management Action Plan

Finding 1 – Established Fraud and Serious Organised Crime Arrangements

Finding Rating	High Priority

Review of the Council’s Fraud and Serious Organised Crime (SOC) arrangements highlighted:

1. The Council does not have a clear fraud, SOC, and AML strategy and plan that covers both operational and cyber fraud.
2. The Council’s fraud prevention policy is dated 2013. Review of the current policy confirmed that:
   - the policy refers to the Council’s Monitoring Officer as having overall responsibility for the policy. This is incorrect and reflects historic structures where the Director of Corporate Governance (who was also the Council’s Monitoring Officer) had overall policy responsibility and the Head of Finance, as one of their direct reports, was the policy owner. The references require updating to refer to the Director of Corporate Services.
   - it states that the Council’s Internal Audit (IA) service plays an important role in the prevention and detection of Fraud. This suggests that IA has responsibility for ownership of key operational fraud prevention controls, which is incorrect and does not support IA independence. This reference is also included in the Anti-Money Laundering Policy.
   - it states that the Council’s financial and non-financial systems are also independently monitored by Internal Audit. This suggests that Council systems are reviewed by IA on an ongoing basis, which is not aligned with the risk based annual IA plan and does not recognise the role of External Audit.
   - it does not provide detail on the significance of frauds (e.g. value and impact) that should be escalated to senior management.
3. The Council’s anti-bribery policy is dated 2015. Review of this policy and the supporting anti-bribery procedure confirmed that they refer to historic risk management procedures, and risk management officers in directorates /services who are no longer in post.
4. Clearly defined fraud and SOC roles, responsibilities, and accountabilities for first line services and the second line framework owners and assurance teams have not been established. In addition, work is required to understand potential key-person dependencies to ensure there are adequate resources and deputising arrangements to for oversight during absence periods as required.

   It is acknowledged that the fraud prevention policy includes a generic statement that directors are responsible for the prevention and detection of fraud, the ant-bribery policy includes clearly defined responsibilities, and the Council’s Response to Serious Organised Crime Group has responsibility to oversee compliance with Scotland’s Serious Organised Crime Strategy.
5. Processes for consistent recording; collation; and reporting fraud and SOC incidents (including AML) across the Council with reports provided to senior management; directors; and the Corporate Leadership Team (CLT) on total incident volumes and their nature and impact (including financial losses) have not been established.
6. A system that supports ongoing recording of fraud, SOC, and AML incidents across Council services is not in place.
7. There is limited information available for services on how to mitigate; identify; manage; address; and report on fraud and SOC incidents.
8. There is limited ongoing assurance on the adequacy and effectiveness of specific fraud and SOC training developed by services and delivered to employees
9. Fraud and SOC e-learning is not reviewed regularly to reflect the changing external environment; the nature of new and emerging fraud and SOC risks; and AML awareness and reporting requirements.

10. Appropriate information and support for Council employees who could potentially suffer from intimidation, harassment, and internal and / or external pressure to engage in fraud and SOC activities has not been developed.
11. An Information Sharing Protocol relation to 'Data washing/Data Sharing' has been drafted and provided to Police Scotland, however feedback and finalisation is outstanding.
12. It is also noted that the Edinburgh Serious Organised Crime Multi-agency forum (a Police Scotland led group which the Council is a member of) has not met formally since August 2019, with no immediate plans to reinstate these meetings.

    The Corporate Resilience team have advised that this is a known issue across a number of local authorities and there have been several requests

Risks

- **Governance and Decision Making** - Fraud and SOC control weaknesses are not identified and addressed through assurance processes, and fraud and SOC incidents and potential incidents are not reported and managed appropriately, with no corporate view of the nature and impact of incidents impacting the Council.
- **Fraud and Serious Organised Crime** – lack of clarity across the Council on frauded and SOC roles, responsibilities, and accountabilities.
- **Workforce** – employees may not be adequately protected from intimidation, harassment, and internal and / or external pressure to engage in fraud and SOC activities.

Recommendations and Management Action Plan –Fraud and Serious Organised Crime Arrangements

Recommendation 1	Agreed Management Action / Implementation Date	Owner/ Lead Officers
The Council's fraud and SOC arrangements should be reviewed, this should include: • update of relevant policies and development of an overarching framework which gives consideration to the issues noted above and is aligned with Audit Scotland expectations on public body counter-fraud arrangements • agreement for where overall responsibility for the framework should sit. Given the current structure of Council and recognition that associated risks are largely related to financial impacts, overall ownership by Finance may be appropriate with support from Corporate Resilience, ultimately this is management's decision.	**1.1 Phased Implementation Plan** **Implementation date:** 30/11/2023 **1.2 Formalise governance arrangements and finalisation of the framework** The SOC working group will work to formalise and gain approval of governance arrangements including establishing clearly documented roles and responsibilities. The SOC working group will also develop and finalise the framework. **Implementation date:** 31/03/2025 1.3 Review and update Fraud Prevention Policy The Fraud Prevention Policy will be reviewed, and the points raised considered as part of the review. **Implementation date:** 31/03/2025	**Owner:** Executive Director of Corporate Services **Lead Officers:** Service Director – Finance and Procurement Service Director – Legal and Assurance Service Director – Human Resources Head of Democracy, Governance and Resilience Corporate Resilience Manager

Recommendation 1	Agreed Management Action / Implementation Date	Owner/ Lead Officers
• formal agreement from Police Scotland on information sharing and future arrangements for the Edinburgh Multi-Agency Serious Organised Crime Board • it is also recommended that the framework is aligned to implementation of the planned Governance and Assurance model to ensure that appropriate and proportionate ongoing first and second line assurance is provided on fraud (including cyber fraud) and SOC high risk services that are most likely to be impacted.	**1.4 Review and update of Anti-Bribery Policy** The policy will be reviewed as recommended. **Implementation date:** 31/03/2025 **1.5 Development of training and awareness programme** A training and awareness programme will be developed with support from the Council's Digital Service who facilitates mandatory cyber training platform, subject matter experts and support from the Council's communications team. **Implementation date:** 31/10/2025	**Owner:** Executive Director of Corporate Services **Lead Officers:** Service Director – Finance and Procurement Service Director – Legal and Assurance Service Director – Human Resources Head of Democracy, Governance and Resilience Corporate Resilience Manager

Finding 2 – Risk Management – Fraud and SOC

Finding Rating	Medium Priority

Risk identification and reporting

The Council's current risk profile includes Fraud and SOC as a key risk category which is reviewed and reported to CLT and Committee. Whilst this includes consideration of high-level associated risks and impacts at a directorate level, there is no established process in place to identify; record; assess; escalate; and manage thematic service fraud and SOC risks across the Council. The Corporate Resilience team raised this through previous discussions with Corporate Risk Management (circa 2019) who advised that risk management work and recording of relevant risks should be performed within individual service areas.

Completion of the annual fraud and SOC checklist (produced by SOLACE, a consulting local government group) is the responsibility of the Council's SOC group and supports identification of thematic risks, however the checklist was last completed in full in July 2019. Management advised that work to update the checklist in commenced in July 2020, however it was not completed due to Covid-19.

It is acknowledged that implementation of the Council's refreshed risk management framework should enable production of consolidated risk reporting to inform the Corporate Leadership Team and Governance, Risk, and Best Value Committee on thematic fraud and SOC risks, and support comparison between the current fraud and SOC risk profile and the Council's agreed risk appetite. It does however remain the responsibility of services to ensure that relevant risks are recorded.

Risks

- **Governance and Decision Making** - The Council's fraud, SOC and AML risks are not effectively identified and managed.

Recommendations and Management Action Plan – Risk Management: Fraud and SOC

Recommendation 2	Agreed Management Action / Implementation Date	Owner/ Lead Officers
Development of the framework at recommendation 1.1 should include engagement with the corporate risk management team to ensure processes are established to identify; assess; and record thematic fraud; serious organised crime (SOC) and anti-money laundering (AML) risks across Council services. In addition, the annual SOLACE fraud and SOC checklist should be completed, and results reviewed by the Council's SOC group. Any gaps identified should be recorded in the CLT risk register, with mitigating actions and implementation timeframes agreed and implementation progress monitored.	This will be a key part of the newly established Corporate Risk Team work programme, advice and support will be provided via guidance and workshops with opportunity to discuss. A copy of the workshop pack will be provided to demonstrate this once finalised. **Implementation date:** 31/10/2024	**Owner:** Executive Director of Corporate Services **Lead Officers:** Service Director – Legal and Assurance Corporate Resilience Manager Head of Health and Safety and Risk Chief Risk Officer

Appendix 1 – Assurance Definitions

Overall Assurance Ratings	
Substantial Assurance	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and the Council's objectives should be achieved.
Reasonable Assurance	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and the Council's objectives should be achieved.
Limited Assurance	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that the Council's objectives should be achieved.
No Assurance	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with a number of significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that the Council's objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.