COUNTER FRAUD CONTROLS ASSESSMENT 2022/23

Report by Chief Officer Audit and Risk

AUDIT COMMITTEE

13 February 2023

1 PURPOSE AND SUMMARY

1.1 **The purpose of this report is to make the Audit Committee aware of the findings and necessary actions arising from the Integrity Group's assessment of counter fraud controls.**

1.2 The Council is committed to minimising the risk of loss due to fraud, theft, corruption or crime and to taking appropriate action against those who attempt to defraud the Council, whether from within the authority or from outside. Tackling fraud is not a one-off exercise; it is a continuous process across all parts of the Council because the service delivery processes it underpins are continuous. Tackling fraud is an integral part of good governance within the Council, safeguarding the Council's resources for delivery of services, as part of protecting the public purse.

1.3 The primary responsibility for the prevention, detection and investigation of fraud rests with Management, supported by the Integrity Group, whose purpose is to improve the Council's resilience to fraud, theft, corruption, and crime. One way it can achieve that is self-assessing the Council's arrangements against best practice and agreeing any appropriate actions to continuously improve the arrangements in place.

1.4 Part of the Audit Committee's role is to oversee the framework of internal financial control including the assessment of fraud risks and to monitor counter fraud strategy, actions and resources.

1.5 Assurances about the effectiveness of the Council's existing systems and arrangements for the prevention, detection and investigation of fraud can be taken from the outcomes contained within this report.

2 RECOMMENDATIONS

2.1 I recommend that the Audit Committee:

a) Acknowledges the findings from the Integrity Group's assessment of counter fraud controls 2022/23 in response to fraud risks; and

b) Endorses the ongoing Management actions to enhance the Council's resilience to fraud, as summarised in the Action Plans set out in Appendices 1 & 2.

3 BACKGROUND

3.1 The size and nature of the Council's services, as with other large organisations, puts the Council at risk of loss due to fraud, theft, corruption, or crime. The Council at its meeting on 16 December 2021 approved a revised Counter Fraud Policy and Strategy 2021-2024, which had been endorsed by the Audit Committee on 22 November 2021. The Council's Counter Fraud Policy states the roles and responsibilities in tackling fraud; the primary responsibility for the prevention, detection and investigation of fraud rests with Management. The revised Counter Fraud Strategy will enable the Council to continue to refine its approach to tackling fraud, taking account of reducing resources, with a focus on prevention and detection and promotion of a counter fraud culture across the Council to improve its resilience to fraud.

3.2 Establishing a counter fraud culture is fundamental to ensuring an effective response to fraud, theft, corruption, or crime and the leadership part played by the Council Management Team (CMT) and Senior Management is key to establishing counter fraud behaviours within the organisation, its partners, suppliers and customers.

3.3 Tackling fraud is not a one-off exercise; it is a continuous process across all parts of the Council because the service delivery processes it underpins are continuous. Tackling fraud is an integral part of good governance within the Council, safeguarding the Council's resources for delivery of services, as part of protecting the public purse.

3.4 The Integrity Group is an officer forum, chaired by the Chief Officer Audit & Risk, which has 2 Director representatives from CMT and representatives from HR, Finance, Legal, IT, and Procurement to support Management to fulfil their responsibilities in tackling fraud. Its purpose is to improve the Council's resilience to fraud, theft, corruption, and crime. It oversees the counter fraud policy framework, agrees and monitors the implementation of counter fraud improvement actions, raises awareness as a method of prevention, and performs self-assessment checks against best practice.

3.5 Internal Audit is required to give independent assurance on the effectiveness of processes put in place by Management to manage the risk of fraud.

3.6 Part of the Audit Committee's role is to oversee the framework of internal financial control including the assessment of fraud vulnerabilities and to monitor counter fraud strategy, actions and resources.

3.7 The Integrity Group carried out assessments in 2020/21 and 2021/22 of counter fraud controls associated with the covid-19-emerging-fraud-risks. The findings from which were reported to the Audit Committee on 8 March 2021 and 14 February 2022 respectively, along with the necessary actions to enhance the Council's resilience to fraud, theft, corruption, and crime.

3.8 The Audit Committee on 12 September 2022 considered the Audit Scotland report 'Fraud and Irregularity Update 2021/22' (link) (published 14 July 2022) that set out a summary of the cases of fraud and other irregularities at public bodies reported by external auditors for the financial year 2021/22. The Audit Committee endorsed the tasks being undertaken by the Integrity Group associated with the Audit Scotland report and requested an assurance report thereon.

4 SELF-ASSESSMENT 2022/23 FINDINGS AND NECESSARY ACTIONS

4.1 One way to improve the Council's resilience to fraud, corruption, theft and crime is through engaging with national forums to share intelligence, lessons learned and best practice, carrying out a self-assessment of the Council's arrangements and agreeing any appropriate actions to continuously improve the arrangements in place.

4.2 The Chief Officer Audit & Risk disseminated the Audit Scotland report 'Fraud and Irregularity Update 2021/22' to the Integrity Group on 3 August 2022 to progress the Actions arising from this report.

4.3 One of the actions arising from the Audit Scotland report 'Fraud and Irregularity Update 2021/22' is for public bodies to consider whether the risks and weaknesses in controls identified in this report may exist in their organisation and taking appropriate corrective actions. Each of the case studies were assigned to the relevant officer to set out the fraud risk controls in place at Scottish Borders Council and to determine whether any Management Actions are required to enhance those controls.

4.4 The Integrity Group on 3 October 2022 reviewed the status of Actions (set out in Appendix 1) and considered the consolidated 'Case Studies Fraud Risk Controls Assessment' (set out in Appendix 2).

4.5 Assurances about the effectiveness of the Council's existing systems and arrangements for the prevention, detection and investigation of fraud can be taken from the outcomes contained within this report. The Integrity Group will continue to monitor progress with implementation of Actions, noting that some are continuous across all parts of the Council.

5 IMPLICATIONS

5.1 **Financial**
Effective internal control systems are designed to prevent and detect fraud, theft, corruption or crime and this contributes to safeguarding the Council's resources for delivery of services, as part of protecting the public purse.

5.2 **Risk and Mitigations**
The process of identifying fraud risks by Management is based on the principles of the Council's Counter Fraud Policy and Strategy. Evaluation and monitoring of fraud risks and mitigations are facilitated through the Integrity Group.

5.3 **Integrated Impact Assessment**
Equality, diversity and socio-economic factors are accommodated by way of all alleged frauds being investigated and pursued in accordance with the appropriate legislation. There is no relevance to Equality Duty or the Fairer Scotland Duty for this report. An Integrated Impact Assessment (IIA) was completed as part of the revised Counter Fraud Policy and Strategy 2021-2024, approved by Council on 16 December 2021. This is a routine good governance report for assurance purposes.

5.4 **Sustainable Development Goals**
The recommendations in this report will not directly impact any of the 17 UN Sustainable Development Goals, based on completion of the checklist as part of the revised Counter Fraud Policy and Strategy 2021-2024. However, the application of practices associated with the Council's Counter Fraud

Policy and Strategy is fundamental to ensuring an effective response to fraud, theft, corruption, or crime. This will make a difference to the UN Sustainable Development Goal 16 "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels".

5.5 **Climate Change**
This report does not relate to any proposal, plan or project and as a result the checklist on Climate Change is not an applicable consideration.

5.6 **Rural Proofing**
This report does not relate to new or amended policy or strategy and as a result rural proofing is not an applicable consideration.

5.7 **Data Protection Impact Statement**
There are no personal data implications arising from the content of this report.

5.8 **Changes to Scheme of Administration or Scheme of Delegation**
No changes are required to either the Scheme of Administration or the Scheme of Delegation as a result of the content in this report.

6 CONSULTATION

6.1 The Integrity Group has carried out the counter fraud controls self-assessment 2022/23 and has been consulted on this report as part of fulfilling its role in enhancing the Council's resilience to fraud.

6.2 The Council Management Team, who play a key leadership role in establishing counter fraud behaviours within the organisation, its partners, suppliers and customers, are being consulted on this Report.

6.3 The Acting Chief Financial Officer, Interim Chief Officer Corporate Governance (and Monitoring Officer), Director – People Performance & Change, Clerk to the Council, and Communications team have been consulted on this report and any comments received taken into account.

Approved by

Jill Stacey, Chief Officer Audit and Risk Signature .....

Author(s)

Name	Designation and Contact Number
Jill Stacey	Chief Officer Audit and Risk Tel 01835 825036

Background Papers: Audit Scotland publications on website
Previous Minute Reference: Audit Committee 14 February 2022 and 12 September 2022

Note – You can get this document on tape, in Braille, large print and various computer formats by using the contact details below. Information on other language translations can also be given as well as provision of additional copies.

Contact us at fraud@scotborders.gov.uk

The Recommendations arising from the Fraud and Irregularity 2021/22 report are set out in the following table, along with the status of the Action by the Integrity Group as at 30 November 2022:

Public bodies should ensure effective counter-fraud arrangements are in place. These include:	**Integrity Group Action – Status as at 30 November 2022**
1) having effective governance and oversight arrangements for counter-fraud	The Council's Counter Fraud Policy states the roles and responsibilities in tackling fraud, including Management, Integrity Group and Audit Committee.
2) understanding the current and emerging counter-fraud risks facing the body	The Integrity Group meets quarterly and considers national reports on emerging risks, and gains insights from members' represented on national forums such as Scottish Local Authorities' Investigators Group (SLAIG).
3) regularly reviewing their counter-fraud strategy and counter fraud plan	A revised Counter Fraud Policy and Strategy 2021-2024 were approved by Council in December 2021. The Counter Fraud Strategy 2021-2024 and planned activities were reviewed during the year by the Integrity Group during quarterly meetings. Counter Fraud planned activity and outcomes are reported annually to Audit Committee.
4) regularly assessing and reviewing internal controls and governance arrangements to ensure they remain effective	A Counter Fraud Controls Assessment is carried out at least annually, and outcomes and improvements reported to the Audit Committee.
5) considering whether the risks and weaknesses in controls identified in this report may exist in their organisation and taking appropriate corrective actions	Integrity Group reviewed the 'Case Studies Fraud Risk Controls Assessment' relating to Scottish Borders Council at its meeting on 3 October 2022, in response to the publication of the Fraud and Irregularity Report 2021/22.
6) reviewing the independent reviews and associated recommendations that were commissioned by the Scottish Environment Protection Agency (SEPA) following a ransomware attack on its systems	This work was undertaken with CGI as part of the Counter Fraud Controls Assessment 2021/22 to review the SEPA report and provide assurance that any identified gaps do not exist within the SBC infrastructure. Furthermore, in partnership with CGI a Cyber Security Maturity Assessment (CSMA) was undertaken. The results of the CSMA are were presented to CMT on 25 May 2022. This assessment has delivered recommendations on how to enhance and increase the effectiveness of current controls and identify areas where resilience against persistent threats could be improved.

Appendix 2

The Integrity Group considered the consolidated 'Case Studies Fraud Risk Controls Assessment' relating to Scottish Borders Council on 3 October 2022, as summarised in the following table:

Case Study Fraud Risk	Fraud Risk Controls in place at Scottish Borders Council	Any action required to enhance existing Fraud Risk Controls	Integrity Group Action Owner
Case study one: Pension Fund	The Fund uses the DWP Tell us Once system, where information on pensioners is uploaded on a monthly basis to include new pensioners, with any match reported back to the Fund. In addition to this an annual Life Certificate exercise is carried out for those pensioners who reside out with the United Kingdom. There is also participation in the NFI exercise where details on pensioners are provided for matching.	Consider whether there is merit in carrying out an exercise to capture any potential unreported deaths as highlighted in the case study given the controls that are and have been in place for a number of years. The Fund will need to explore how such an exercise could be carried out, including the costs associated with this.	Director People, Performance & Change
Case study two: Procurement Cards	SBC Purchase Cards are covered by a Policy & Procedure which states the responsibilities of all stakeholders in the purchase card (pCard) process. Training is undertaken by all pCard holders and a Declaration of Agreement (based on understanding of the policy) completed and recorded by the Purchasing Team. Transactional limits are centrally controlled by the Purchasing Team. To agree a change to transaction limits requires approval by the budget holder and CCS team. A record of all requested changes is recorded by the Purchasing Team. Only those in the purchasing service with appropriate RBS SDOL system access can amend card limits. Transactional limits are set up to enable low value/ low risk purchases – the current limits reflect this i.e. no one in the SBC estate would have access to the kind of limit (£7,300) misused in the case study. Transactional data is reviewed monthly as part of the pCard data reconciliation into Business World. Any transactions deemed as potentially inappropriate (i.e. that go against the policy do's and don'ts) are highlighted and an email query sent to the card holder. If a transaction continues to be identified as potentially inappropriate the purchase card is put on stop by the Purchasing Team and the details escalated to line management and/or the budget holder for investigation. pCard limit reviews take place on all cards twice a year and limits adjusted in line with actual use (with consultation with card holders). Any cards found to have not been used are queried and if appropriate accounts closed/ cards cancelled.	Regularly review and update where required the relevant control reconciliation internal guidance (used by the Purchasing Team) – this is ongoing – last update July 2022. Review and update where appropriate the associated Policy & Guidance for card holders – last update Sept 2021 with a planned review update before scheduled Sept 2023. Continue with twice annual card limit reviews.	Financial Services Manager

Case Study Fraud Risk	Fraud Risk Controls in place at Scottish Borders Council	Any action required to enhance existing Fraud Risk Controls	Integrity Group Action Owner
Case study three: Invalid Supplier	Processes to update supplier bank details include verifiable evidence direct from supplier necessary in advance of making any changes. Payments team staff are aware of increased risk and are extra vigilant.	The roll-out of the Supplier Relationship Management module in Business World system, that is well underway, will allow suppliers to access portal to update their bank and other details.	Financial Services Manager
Case study four: Ticket Income	n/a		
Case study five: Covid-19 Funding	The approach taken in Business Grant and Cost of Living Payment work as much as possible and practical has undoubtedly prevented possible fraud and error. The approach taken was cross officer/Team working within CASS bringing together various areas and depth of experience and knowledge plus involving other resources from outside CASS e.g. Finance, which meant a better preventative position from the start.	Ongoing to maintain that collaborative approach as new things arise since its seems to focus minds and have the best scope for reducing opportunities for fraud. The cheque and payment cards discussions are a current example of the joined up approach being applied in practice.	Director Resilient Communities
Case study six: Covid-19 Funding	As above	As above	Director Resilient Communities
Case study seven: IT and cybercrime	**User Awareness** Continued periodic emails are distributed regularly reminding staff of their responsibilities and guidance on what to do if a Spam/Phishing email is received. A short life working group has been setup with elected members to increase awareness. IT Client Manager and SBC Enterprise Architect attends both Scottish Local Authority Information Security Group (SLAISG) and Scottish Government Public Sector Cyber Resilience Network quarterly meetings. **Cyber Security Maturity** In partnership with CGI a Cyber Security Maturity Assessment (CSMA) was undertaken. The approach to this was underpinned by a range of methodologies including: NCSC's cyber risk management guidance, NCSC Cyber Assessment Framework, ISO27001. The results of the CSMA were presented to the Council Management Team on 25 May 2022. This assessment has delivered recommendations on how to enhance and increase the effectiveness of current controls and identify areas where resilience against persistent threats could be improved. Guidance from NCSC Actions to take when cyber threat is heightened are being reviewed regularly.	Regular and evolving security awareness training for staff/users across all levels of the organisation, delivered in various methods to ensure engagement and ownership Council Management Team to review and agree plan of action for implementation of recommendations from the CSMA. Paper being presented to aid discussion and decision-making process.	IT Client Manager