COUNTER FRAUD CONTROLS ASSESSMENT

Report by Chief Officer Audit & Risk

AUDIT AND SCRUTINY COMMITTEE

8 March 2021

1 PURPOSE AND SUMMARY

1.1 **The purpose of the report is to make the Audit and Scrutiny Committee aware of the findings and necessary actions arising from the Integrity Group's assessment of counter fraud controls associated with the covid-19-emerging-fraud-risks.**

1.2 The Council is committed to minimising the risk of loss due to fraud, theft or corruption and to taking appropriate action against those who attempt to defraud the Council, whether from within the authority or from outside.

1.3 The primary responsibility for the prevention, detection and investigation of fraud rests with Management, supported by the Corporate Fraud and Compliance Officer. Internal Audit provides advice and independent assurance on the effectiveness of processes put in place by Management. Part of the Audit and Scrutiny 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.

1.4 The Audit and Scrutiny Committee at its meeting on 28 September 2020 requested that the Corporate Fraud Steering Group (Integrity Group) of officers consider all three Audit Scotland counter fraud reports as part of their counter fraud role and responsibilities, and carry out an assessment of counter fraud controls associated with the covid-19-emerging-fraud-risks and report back to the Committee on findings and necessary actions at the earliest opportunity. This report fulfils that decision.

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 and Scrutiny Committee:

a) Acknowledge the findings from the Integrity Group's assessment of counter fraud controls associated with the covid-19-emerging-fraud-risks; and

b) Endorse the necessary actions to enhance the Council's resilience to fraud, as set out in the relevant sections in the body of the report and summarised in the Action Plan in Appendix 1.

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 or corruption. 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.

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 Corporate Management Team and Senior Management is key to establishing counter fraud behaviours within the organisation, its partners, suppliers and customers.

3.3 The Corporate Fraud Steering Group (Integrity Group) is a forum which has representatives from across the Council's Services to support Management to fulfil their responsibilities in tackling fraud. Its purpose is to improve the Council's resilience to fraud, corruption, theft 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.

3.4 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 and demonstrates effective financial stewardship and strong public financial management.

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 and Scrutiny 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 Audit and Scrutiny Committee at its meeting on 28 September 2020 considered three counter fraud reports published by Audit Scotland in June and July 2020, including one on Covid-19 emerging fraud risks:

https://www.audit-scotland.gov.uk/report/covid-19-emerging-fraud-risks

The Audit and Scrutiny Committee requested that the Corporate Fraud Steering Group (Integrity Group) of officers consider all three Audit Scotland counter fraud reports as part of their counter fraud role and responsibilities, and carry out an assessment of counter fraud controls associated with the covid-19-emerging-fraud-risks and report back to the Committee on findings and necessary actions at the earliest opportunity.

4 SELF-ASSESSMENT FINDINGS AND NECESSARY ACTIONS

4.1 The Audit Scotland report on emerging public sector fraud risks due to Covid-19 was structured within categories. The findings of the Integrity Group's assessment of Scottish Borders Council's counter fraud controls and necessary actions are set below using those categories.

4.2 **General governance risk**

Existing controls in the Council's main business applications, including the Business World ERP system, remained applicable with the shift to remote working.

Supervision and training was provided by host Services for deployed staff.

Internal Audit staff working from home; none were redeployed. Audits were added to the Plan to carry out assurance work on new risks associated with the Covid-19 emergency response. Adjustments to the Internal Audit Plan were discussed with SMTs then CMT and approved by the Audit and Scrutiny Committee 24 November 2020, covering sufficient range and breadth of audit activity to provide the statutory audit opinion.

4.3 Procurement risk

Processes to update supplier bank details remain the same as pre-Covid with verifiable evidence direct from supplier necessary in advance of making any changes, with a minor adjustment used on a few occasions where companies have no physical presence at offices (digital rather than paper-based, in consultation with Internal Audit). Payments team staff are aware of increased risk and are extra vigilant.

Business World ERP system and associated invoice approval workflows provides a digital route from the ordering of goods and services through to payment of suppliers. Internal controls are inbuilt into the systems and associated workflows.

Procurement team worked closely with suppliers, Scotland Excel and other public sector colleagues to protect the supply chain. Use made of the provisions in Regulation 72 of the Public Contracts (Scotland) Regulations 2015 and the Council's waiver procedure to modify and extend existing contracts, where appropriate, to avoid disrupting the supply of goods and services.

Internal controls are inbuilt into the Business World ERP system and associated workflows, including checks to both prevent and identify duplicate payments. Receipting of goods and services is part of the workflow prior to payment of suppliers. Duplicate payments are detected through participation in the National Fraud Initiative exercise using data matches from a variety of data sets.

Required Procurement procedures were maintained and monitored. There has been extra vigilance by the Trading Standards team on product supplies in the area.

Further actions in this area include:

- A development, as part of improvements to the Council's contract management arrangements, is the roll-out of the Supplier Relationship Management module in the Business World system which will allow suppliers to access the portal to update their bank and other details.
- Internal Audit carry out annual review of Business World key controls.

4.4 Covid-19 funding

The legislation surrounding the Business Support Grants was very complex and intricate and introduced over a number of phases which brought about changes that had to be incorporated into processes quickly to allow payments to be made in a timely manner. Procedures and policies were documented and updated as legislation changed. Staff reacted quickly to a unique, fast changing situation to allow payments to be made to businesses in need. Staff are vigilant in applying checks to prevent fraudulent payments being made.

Community Councils were provided with funds to assist households in immediate need to buy food and essential items.

Weekly reporting of stats were submitted to Scottish Government.

Further actions in this area include:

- Learning lessons from initial phases to apply to new specific Covid-19 grant funding being administered on behalf of the Scottish Government.
- Ongoing staff vigilance on checks and controls.
- Ongoing engagement by Internal Audit in SLAIG to keep up to date on areas of fraud, and with Services administering new funds.

4.5 Payroll/recruitment risk

Interviews are carried out virtually. Recruiting Manager verification of the person notified by email. Virtual verification of documents is carried out when preferred candidate is selected prior to commencement of employment. Disclosure Scotland brought forward the implementation for online PVG requests.

No changes in the process for payroll checking and reconciliation. E-forms and workflows were already in place for contractual change notifications, sickness absence notification and COVID related special leave. The process for the submission and processing of timesheets not changed (paper-based for some Services).

Further action in this area include:

- Internal Audit carry out annual review of Business World key controls.

4.6 IT/Cybercrime risk

There are periodic emails reminding staff of their responsibilities on data and information security, of the MyIT Self Service Portal to raise system issues with CGI, and about phishing emails and how to report them.

USB devices need to be on the Anti-Virus whitelist to work. Once on the whitelist, staff only have read access until Bitlocker encrypts the USB.

The Council employs a defence in depth approach that includes a series of technical and organisational controls to prevent such a cyber attack (PSN and Cyber Essentials accreditation).

SBC/CGI receive Crew notices/threat intelligence relating to public sector potential and actual cyber crime attacks. Staff can be made aware quickly about emerging threats.

The Information Governance Group meets quarterly to monitor and review information risks, policies and procedures, data breaches and security incidents, and the completion of e-learning including GDPR, to ensure actions are taken in response to issues. There are periodic emails reminding staff of their responsibilities. A number of business applications maintain audit trails of access that can be reviewed by Managers.

Further actions in this area include:

- Continued periodic emails reminding staff of their responsibilities, and guidance on what to do.
- Ongoing monitoring of the effectiveness of the technical and organisational controls. Ransomware attacks are becoming extremely sophisticated; delivery mechanisms (such as email) are bypassing technical and filtering controls by using Morse code to create malicious URL links. More focus is required on staff/user security awareness/education.

4.7 Health and wellbeing risk

Staff communications include weekly staff update emails that provide guidance, support and information on the response and recovery activity, remote working, and other safe systems of work.

A range of wellbeing supports includes provision of a mix of formal and informal offerings to support the wellness of its employees, ranging from occupational health, people policies, themed events, training, helplines and other support. Supervision and training provided by host Services for deployed staff.

Message to staff on their responsibilities for Protecting the Public Purse as well as information on how to raise concerns via the whistleblowing process.

Further action in this area includes:

- Ongoing staff and other stakeholder communications to remind them of the wellness supports that are available, and ongoing supervision and training.

4.8 Wider risks

Public awareness campaigns from the Scottish Government, Action Fraud, NCSC and others alert people to the dangers. These will continue alongside Covid-19 response and recovery phases.

Further action in this area includes:

- Ongoing cascading of public awareness campaigns via staff and other stakeholder communications.

5 IMPLICATIONS

5.1 Financial

Effective internal control systems are designed to prevent and detect fraud and this contributes to safeguarding the Council's financial resources, for delivery of services, as part of protecting the public purse. Any additional costs arising from enhanced fraud risk mitigation will have to be considered and prioritised against other pressures in the revenue budget.

5.2 Risk and Mitigations

The process of identifying fraud risks is based on the principles of the Corporate Risk Management Policy and Framework. Evaluation and monitoring of fraud risks and mitigations are facilitated through the Corporate Fraud Steering Group (Integrity Group), and regular communications and training are offered. Oversight is provided by the Audit and Scrutiny Committee.

The Integrity Group's assessment of counter fraud controls associated with the covid-19-emerging-fraud-risks contained in this report is designed to provide assurance to Management and the Audit and Scrutiny Committee on the efficacy of Scottish Borders Council's arrangements, and sets out the actions that are ongoing or required to enhance the Council's resilience to fraud.

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. This is a routine good governance report for assurance purposes, not a new or revised policy or strategy for decision and, as a result, completion of an Integrated Impact Assessment is not an applicable consideration.

5.4 **Acting Sustainably**

There are no direct economic, social or environmental issues with this report.

5.5 **Carbon Management**

There are no direct carbon emissions impacts as a result of this report.

5.6 **Rural Proofing**

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

5.7 **Changes to Scheme of Administration or Scheme of Delegation**

No changes to the Scheme of Administration or Scheme of Delegation are required as a result of this report.

6 CONSULTATION

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

6.2 This report has been presented to the Corporate Management Team, who play a key leadership role in establishing counter fraud behaviours within the organisation, its partners, suppliers and customers. Notably requesting the inclusion of the summary Action Plan in the Appendix 1.

6.3 The Executive Director Finance & Regulatory, Chief Legal Officer (and Monitoring Officer), Service Director HR and Communications, Clerk to the Council, and the Communications team have been consulted on this report and any comments received have been incorporated.

Approved by

Jill Stacey **Signature .....**
Chief Officer Audit & Risk

Author(s)

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

Background Papers: Scottish Borders Council's Counter Fraud Policy Statement and Counter Fraud Strategy
Previous Minute Reference:

Note – You can get this document on tape, in Braille, large print and various computer formats by contacting the address below. The Audit & Risk Service can also give information on other language translations as well as providing additional copies.

Contact us at fraud@scotborders.gov.uk

Appendix 1

Risk Area	Action required to enhance existing Fraud Risk Controls	Integrity Group Action Owner	Target Date
Procurement	The roll-out of the Supplier Relationship Management module in Business World system will allow suppliers to access portal to update their bank and other details.	Commercial & Commissioned Services Manager	April 2021
	Internal Audit carry out annual review of Business World key controls.	Chief Officer Audit & Risk	March 2021
Covid-19 Funding	Learning lessons from initial phases to apply to new specific Covid-19 grant funding being administered on behalf of the Scottish Government.	Service Director Customer & Communities	Ongoing in new phases
	Ongoing staff vigilance on checks and controls.	Service Director Customer & Communities	Ongoing in new phases
	Ongoing engagement by Internal Audit in SLAIG to keep up to date on areas of fraud, and with Services administering new funds.	Chief Officer Audit & Risk	September 2021
Payroll-Recruitment	Internal Audit carry out annual review of Business World key controls.	Chief Officer Audit & Risk	March 2021
IT-Cyber Crime	Continued periodic emails reminding staff of their responsibilities, and guidance on what to do.	IT Client Manager	Monthly/quarterly
	Ongoing monitoring of the effectiveness of the technical and organisational controls. Ransomware attacks are becoming extremely sophisticated; delivery mechanisms (such as email) are bypassing technical and filtering controls by using Morse code to create malicious URL links. More focus required on staff/user security awareness/education.	IT Client Manager	Ongoing
Health & Wellbeing	Ongoing staff and other stakeholder communications to remind them of the wellness supports that are available, and ongoing supervision and training.	Service Director HR & Communications	Fortnightly
Wider Risk	Ongoing cascading of public awareness campaigns from the Scottish Government, Action Fraud, NCSC and others to alert people to the dangers via staff and other stakeholder communications.	Service Director HR & Communications	Monthly/quarterly