ARGYLL AND BUTE COUNCIL **AUDIT AND SCRUTINY COMMITTEE**

FINANCIAL SERVICES **14 SEPTEMBER 2021**

AUDIT SCOTLAND - 2020/21 FRAUD AND IRREGULARITY REPORT

1.0 INTRODUCTION

1.1 This report provides the Audit and Scrutiny Committee (the Committee) with reassurance that the Council has appropriate governance and counter fraud arrangements in place to mitigate, as far as possible, the risks highlighted in Audit Scotland's 'Fraud and Irregularity 2020/21' report.

2.0 RECOMMENDATIONS

2.1 Endorse this report and note the assurance that the Council has robust policy and procedures to, as far as possible, mitigate the risks identified in Audit Scotland's 2020/21 Fraud and Irregularity Report.

3.0 DETAIL

Audit Scotland Report

3.1 In July 2021 Audit Scotland published a report titled 'Fraud and Irregularity 2020/21' with the purpose of sharing risks and case studies to support the Scottish Public Sector in the prevention of fraud. The reports overarching recommendation was that public bodies should ensure good governance and counter fraud arrangements are in place including:

- Having appropriate governance and oversight arrangements for counter fraud
- Regularly reviewing controls and governance arrangements to ensure they remain fit for purpose
- Being alert to emerging fraud risks and where appropriate working with others to help alleviate there risks
- Considering whether the council has appropriate controls in place to prevent the risks identified in the Fraud and Irregularity report materialising
- Considering whether the weaknesses in internal control that facilitated the fraud or irregularity identified in the report may also exist in the council.

3.2 The report grouped fraud related risk into seven categories. Full details of the associated risks in each category are detailed on pages 6-12 of the Audit

Scotland Report included as Appendix 1 to this paper however the table below summarises them and the Council's position in relation to them

Category	Summary of Associated Risks	Council Position
COVID Funding and Recovery	• Government funding provided quickly possibly with limited scrutiny/due diligence • Fraudulent attempts to access eligible business information to use as part of a fraudulent application • Requests to change business rates information to qualify for grants • Provision of fraudulent documents to support grant applications • Malware attempts purporting to be from recognised bodies	The risk of fraud was an ongoing consideration by all officers processing grants. Information on suspected fraudulent claims was shared across all Scottish Local Authorities and officers applied professional judgement and expertise when assessing applications to identify indications that an application may be fraudulent. In the event that any indications were identified further due diligence was performed to robustly confirm the validity of the application. Ongoing evolution of grant administration processes, including refining online application forms, assessment checklists, new communication platforms and best practice sharing. Internal Audit officers were involved in the administration of the Council's SBGF, RHLGF and Discretionary Fund and the Chief Internal Auditor was the appeal officer for the SBGF, RHLGF, Discretionary Fund grants and Taxi Grants. As such Internal Audit played an active role in the design of the processes adopted to administer business support funds - this is considered to provide greater assurance than a retrospective audit after the event.

		The Council's more routine processes in relation to standing data change requests were not altered during the COVID response and these are subject to continuous monitoring by internal audit.
Health and wellbeing	• Staff remote working may lead to isolation, mental health issues and/or increased addictive behaviours increasing vulnerability to organised crime • Increase in internal fraud due to staff feeling financial and health pressures. • Working for sustained periods at high pace or pressure may lead to errors • Phishing emails sent to staff offering, for example, free Covid vaccines. Often such emails ask to confirm bank details.	The Council were, and still are, very conscious of mental health issues associated with remote working. Wellbeing services have been promoted via all staff e-mails and the staff website. Furthermore managers have been regularly encouraged to ensure communication channels with staff are maintained. Where officers have found homeworking challenging the option of working from an office has been made available. In light of offices reopening, there will be scope for some staff to return to a more 'normal' working pattern and, to support this, staff surveys have been issued to ensure staff opinions are factored in to any decision making.
IT & Cybercrime	• Staff working remotely may pose potential security risk when using personal devices and/or removable devices to download data • Household members may gain access to confidential information by looking at screens or hard documents.	Argyll and Bute Council was the first UK council to implement and utilise Skype for Business in 2010 and meaning staff were already well equipped to work flexibly from multiple locations. As a result council staff seamlessly transitioned from working in the office to working from home at the beginning of the pandemic. Furthermore the Council's IT infrastructure was updated and has coped well with the additional

	• Staff may be more likely to steal or tempted to steal data without the usual office environment and supervision. • Remote working staff may receive bogus calls from fraudsters claiming to be legitimate IT departments or broadband providers attempting to gain access to systems. • Risk of cybercrime when public sector staff connect remotely to access systems for meetings • Risk of ransomware attacks. • Major issue with Phishing emails. Most staff are now remote working and most data transfer is electronic. Staff are heavily dependent on IT and systems. Fake emails and requests for log in details are abundant	pressure brought about by mass remote working. All information required by staff are held on our secure network and security measures are in place which prevent staff connecting removable devices to their work laptops. Phishing training and awareness is available on our HUB (during and prior to COVID) and the Council has an ICT compliance and security officer. During the lockdown the Council had the UK's highest level of cyber security accreditation (Cyber Essentials Plus) which evidences our commitment to protecting data against the most common internet-based threats to cyber security. These include hacking, phishing and password guessing. This expired in June 2021 and the Council are resubmitting their accreditation application shortly with an expectation this will be approved by September 2021. The Council is also PSN (Public Service Network) accredited which confirms the Council's IT security arrangements, policies and controls are sufficiently rigorous for the Council to be allowed to interact with the PSN and those connected to it.
Governance	• Public sector staff working remotely and	Internal audit staff were redeployed to work on business

	under pressure may mean internal controls are relaxed • Buildings being closed results in additional risk of security • New equipment and IT devices purchased during the pandemic needing tagged and sent to remote staff. • Staff transferring to new departments to meet operational needs • Risk of weakened governance arrangements due to internal audit teams being redeployed	support grants for a period of approximately three months however a revised audit plan was still delivered with some 'lost' time backfilled by an agency worker. Transactional controls in key processes are subject to continuous monitoring by internal audit and, since that work recommenced post redeployment there is no evidence that controls were relaxed during remote working. Whilst some buildings have been closed, there has been ongoing presence in the main Council offices, and there have been no notable security issues. Staff were redeployed where necessary however this was overseen by HROD and managed effectively. The Council did revise its governance arrangements in response to COVID which were assessed by Audit Scotland as part of their 2019/20 annual audit. They concluded that in the Council's annual audit report that '*The new arrangements are appropriate and support good governance and accountability.'*
Procurement	• Controls may be relaxed to all the Council to purchase goods or services urgently, possibly from new and untested suppliers. • Sale of items may be at inflated prices, may be counterfeit or	The majority of the Council's purchases are made through PECOS which has established procedures and controls. These controls were not relaxed during COVID as they are largely system controls rather than manual ones. Larger scale procurement is overseen by the Council's

	products not fit for purpose • Fraudulent communication regarding delivery of products. Invoice not paid yet or demands for extra shipping fees. Phishing emails or malware can be included.	procurement team which continued to operate 'business as usual' throughout the pandemic.
Payment	• Duplicate or erroneous payments being made from fraudulent requests from suppliers to change supplier details when staff are under pressure • Goods not being checked by purchase staff for suitability or quality checks before being given to front line staff. • Approval of payments above authorisation limits • Phishing communications received asking for payees to be added, bank account changes, or other changes that in doing so provides personal information.	Authorisation limits for payments were not altered during COVID and controls relating to potential duplicate payments and changes to supplier standing data have not been relaxed during remote working. During the COVID response all invoices were paid immediately with the standard 30 day terms relaxed however all the usual audit checks were still carried out prior to payment. Payment controls are subject to Internal Audit's continuous monitoring programme and will continue to be assessed on an ongoing basis.
Payroll and Recruitment	• Rapid recruitment of staff as operational demand increases –	The Council recruit using MyJobScotland as a platform. There has been no changes to

	normal checks not completed • Payroll fraud may increase as controls over working hours, expenses or overtime might slip. • Fraudulent communications regarding the HSCP £500 "thank you" payment • Fraudulent communications regarding National Insurance and HMRC tax refunds number errors and details required to update/renew • Fake Covid19 job adverts on social media. Phishing for personal details through online applications	our recruitment processes during COVID and all necessary checks are completed prior to recruiting an employee. Expenses have been at a minimal during COVID due to very limited need for travel and subsistence however where they are incurred they are still subject to manager approval through My View. The risk of fraudulent communications is somewhat mitigated by the measures detailed above in the IT and Cybercrime section.

Further Assurance

3.3 In addition to the measures detailed in exhibit 1 further assurance over fraud and irregularity can be taken from the measures explained in the paragraphs below.

3.4 The Council have an established Counter Fraud Team (CFT) who act as a deterrent to fraud and provide a mechanism for investigating potential fraud.

3.5 The Council's Internal Audit team regularly review controls and governance arrangements to ensure they remain fit for purpose and raise recommendations for improvements.

3.6 The CFT and Internal Audit have joint team meetings every fortnight to discuss ongoing and emerging issues. Furthermore the CFT are in regular

communication with the Scottish Local Authority Investigator Group (SLAIG) and have been sharing information and discussing emerging issues.

4.0 CONCLUSION

4.1 The COVID pandemic did increase the risk of fraud for all councils due to the amount of funding made available by the UK and Scottish Government to be distributed to businesses. This inevitably created an opportunity for fraudsters to attempt to access these funds through fraudulent means. Furthermore temporary changes to working practices can always result in routine systems of controls being relaxed. However whilst the Council, like all councils, would have been targeted by fraudsters, fraud it is considered that their existing processes and, any necessary changes to them, or new processes, were implemented and managed appropriately and therefore we were not exposed to an excessive level of risk.

5.0 IMPLICATIONS

5.1 Policy - None
5.2 Financial – None
5.3 Legal – None
5.4 HR - None.
5.5 Fairer Scotland Duty - None
5.5.1 Equalities – None
5.5.2 Socio-Economic Duty – None
5.5.3 Islands Duty - None
5.6 Risk – None.
5.7 Customer Service - None

Laurence Slavin
Interim Head of Financial Services
14 September 2021

For further information contact:
Colin Rae, Counter Fraud Team Lead (01436 657685)

Appendices

Appendix 1 – Audit Scotland 2020/21 Fraud and Irregularity Report