Glasgow City Council Internal Audit Section
Committee Summary
Corporate Review – Information Security Risk Management

Item 3(f)

20th March 2024

1 Introduction

1.1 As part of the agreed Internal Audit plan, we have carried out a review of Information Security (IS) Risk Management.

1.2 In 2021 an independent consultant was commissioned by the Council to examine various aspects of its IS management system. The findings of this audit were reported to the Finance and Audit Scrutiny Committee (FASC) in January 2022 and recommended a series of improvements to enhance the Council's management of IS related risks.

1.3 These included the formation of a single IS risk register to be managed by GCC, more comprehensive risk reporting and analysis, tighter controls around risk acceptance, greater focus on the risk register at the Security Working Group (SWG) as well as the maintenance of an issues log by the group.

1.4 The purpose of this audit was to assess the adequacy of the Council's IS Risk Management processes to ensure that all IS risks are captured on a single register, routinely monitored and reported to the Information Security and Integrity Board (ISIB) on a regular basis.

1.5 The scope of the audit included a review of:

- The IS Risk Register ensuring that it is aligned with the requirements of Council's Corporate Risk Management Policy and Framework.
- The ownership arrangements for the IS Risk Register, ensuring that these have been clearly assigned and understood.
- The mechanisms in place for identifying and recording IS related risks across the Council, including those which are identified by Council contractors, e.g. CGI.
- The adequacy of IS risk management review processes, including the role of the IS risk management sub-group of the ISB.
- The IS risk reporting arrangements, ensuring that the risk register is regularly reported to the ISIB.

2 Audit Opinion

2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and one recommendation which management should address.

3 Main Findings

3.1 We are pleased to report that the key controls are in place and generally operating effectively.

3.2 We confirmed that a single IS Risk Register has been created, which captures risks from multiple sources, and is managed by GCC in line with the Risk Management Policy and Framework. Ownership of this IS Risk Register has been assigned to an appropriate individual. Periodic checks of relevant risk registers are also undertaken to identify IS risks that should be noted on the central register.

3.3 We noted that a new sub-group called the Security Risks and Issues Forum (SRIF) has been introduced, which replaces the IS risk management sub-group. This new group was set up to review and monitor the IS risks and issues across the Council and make recommendations on these to the Senior Information Risk Owner (SIRO), the Information Security and Integrity Board (ISIB) and the Extended Information Security Board (EISB) in order that such risks and issues can be managed appropriately.

3.4 We confirmed that reporting of risk information is standardised and follows the GCC risk management framework.

3.5 However, our audit testing identified some opportunities for improvement.

3.6 For the new SRIF we noted that some aspects in relation to the governance and membership of the group had not been finalised.

3.7 An action plan is provided at section four outlining our observations, risks and recommendations. We have made one recommendation for improvement. The priority of this recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	0
Medium	Less critically important controls absent, not being operated as designed or could be improved.	0
Low	Lower level controls absent, not being operated as designed or could be improved.	1
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

3.1 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.2 We would like to thank officers involved in this audit for their cooperation and assistance.

3.3 It is recommended that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Information Security risks are routinely reported to the appropriate governance forums for scrutiny				
1	We identified two aspects marked as TBC in the SRIF Terms of Reference (ToR) that required finalisation. Not all relevant stakeholders, as specified in the ToR, had been appointed to sit on the Forum and also the quorum of meetings had not been finalised. With key aspects of the ToR not being finalised, the SRIF may not be as effective as it could be.	The SIIT team should ensure that the ToR for the SRIF is finalised in full and approved, including appointing relevant members and also finalising the quorum of meetings.	**Low**	**Response:** Accepted. **Officer Responsible for Implementation:** Head of SIIT **Timescales for Implementation:** 31 March 2024