GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Item 2(e)

28th September 2022

Title of the Audit: Corporate Review – Data Loss Prevention Controls

1. Introduction

1.1 As part of the agreed Internal Audit plan we have carried out a review of Data Loss Prevention (DLP) measures in place across the Council. DLP is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Data loss can occur through a variety of channels, e.g. email, cloud storage, removable media etc. and organisations should have arrangements in place to prevent and detect data loss where possible.

1.2 Each month a DLP report is provided by CGI and presented to all services and ALEO representatives (except Glasgow Life who compile their own reports) at the Information Security Board. This report is a summary of all unprotected outbound e-mail traffic from the Council, that has triggered an alert that is based on pre-set parameters. The report will include any Payment Card Industry (PCI) information (e.g. 16 digit card number) or SWIFT codes used for international banking transactions. If lost, this data could be used to commit fraud against an individual or business, and could also result in regulatory fines and reputational damage to the Council.

1.3 We summarised the data supplied by CGI and found that in 2021, a total of 2,018 e-mails were sent outwith the Council that contained a trigger, which is an average of 168 e-mails per month. These contained a possible 7,012 instances of potential PCI and SWIFT data. On average 73 employees per month were involved in the sending of this data. As noted above, rule-based parameters have been applied to the email system in order to generate these alerts. However this is not 100% accurate and may trigger alerts for data that meets the ruleset but may not actually be PCI / SWIFT data (e.g. GPS coordinates).

1.4 Services, and relevant ALEOs, are required to review the cases reported each period and engage with their operational areas to determine whether the emails are being sent for legitimate business purposes, and if process improvements can be made. Steps should be taken to remove the emailing of payment information from processes, where possible, or ensure that emails containing payment information are at least suitably protected, e.g. via encryption.

1.5 The purpose of the audit was to review services' utilisation of the DLP report to ensure that this was being used effectively to minimise the risk of data being lost via email, as well as other potential exfiltration channels.

The scope of the audit included a review of:

- The policies, procedures, and guidance available, relating to DLP, and staff understanding of these.
- The processes in place across each service for dealing with the monthly data presented and a sample-based review of the action

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – Data Loss Prevention Controls

taken in response to mitigate the risk.

- Technical and procedural controls across other DLP channels, such as removable media and cloud storage.
- Service / Corporate plans for managing data loss.

2. Audit Opinion

2.1 Based on the work carried out a limited level of assurance can be placed upon the control environment. The audit has identified scope for improvement in existing arrangements and 5 recommendations which management should address.

3. Summary

3.1 We found that DLP control improvements could be made in the following key areas:

- Enhanced utilisation of DLP reporting information
- Cloud storage use
- Removable media control and use
- Email and document encryption

3.2 An action plan has been agreed with Council management in which we have made five recommendations for improvement. For security purposes, we have not included the detailed action plan in these papers. The priority of each recommendation is:

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – Data Loss Prevention Controls

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	3
Medium	Less critically important controls absent, not being operated as designed or could be improved.	2
Low	Lower-level controls absent, not being operated as designed or could be improved.	0
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

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

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

3.5 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.