Item 3(c)

8th May 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – Email Auto-Forwarding Arrangements

1. Introduction

1.1 As part of the agreed Internal Audit plan we have carried out a review of email auto-forwarding arrangements across the Council.

1.2 Auto-forwarding rules, if used appropriately, are an effective means of redirecting email to other users when they meet a defined criteria. However, if they are not used in the correct manner there is a risk that personal or sensitive data could leave the Council network. In addition there is a risk that email looping could occur (e.g. where an auto-forwarding rule has been set up to an email account which is issuing auto-responses, thereby continuing to propagate).

1.3 The Council migrated from the Microsoft Outlook email platform to the cloud-based Exchange Online email facility, part of Microsoft Office 365, during 2017/18.

1.4 The scope of the audit was to review the suitability and operational effectiveness of the controls in place for the application and management of auto-forwarding rules. The scope of the audit included:

- A review of the Council's policies and expectations in relation to the use of auto-forwarding rulesets;
- A sample based review of the rulesets currently in use across the Council;
- An assessment of end user compliance with auto-forwarding policy and guidance;
- An examination of any exception processes and the audit trails in support of these, and
- A review of the monitoring processes currently in place to identify where auto-forwarding rules have been incorrectly applied.

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 three recommendations 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. The Council's Information Security policy, which outlines the Council's requirements in relation to the use of auto-forwarding rules, has been clearly documented and communicated via corporate communications, and through information security related training courses.

3.2 The Exchange Messaging Team within CGI (the Council's IT provider) receive alerts when new externally facing rules are created and we were advised that action is taken to remove these in a timeous manner thereafter. In addition the risk posed by email looping has been mitigated somewhat, through the migration to Exchange Online which has increased network capacity, through the cloud. Furthermore, emails have been configured only to generate a limited number of auto-responses in order to prevent looping.

3.3 Through our audit testing we found that there were no instances of auto-forwarding rules that had been set up to send to distribution lists. We also found that some of the larger distribution lists (e.g. #AllCouncil) had been suitably restricted to reducing the likelihood of errant emails being sent to large groups of Council staff.

3.4 However, our audit testing found that there are some areas of non-compliance. Although methods are available, at the time of the audit there were no technical controls applied to prevent users from setting up externally facing auto-forwarding rules. Although this is mitigated through the alerts that Exchange Online generates, we found a total of 192 externally facing rules set up across the Council. We were advised that these are legacy rules (i.e. pre migration to Exchange Online).

3.5 Through sample testing we identified one instance where Council data has left the network via an auto-forwarding rule in place. This related to a procurement project and may have contained commercial information. We confirmed however that the rule has now been removed and that the data has been deleted.

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

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	1
Medium	Less critically important controls absent, not being operated as designed or could be improved.	1
Low	Lower level controls absent, not being operated as designed or could be improved.	1

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

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

3.9 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.

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – Email Auto-Forwarding Arrangements

4. Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Rules on the use of auto-forwarding have been clearly defined, communicated and understood.				
1	Although the Council has clearly outlined its requirements in relation to the use of auto-forwarding, we found 192 externally facing rules in place across 97 different users. The use of external auto-forwarding is prohibited under Council Policy. Through discussions with users who had set up auto-forwarding rules there was a lack of understanding in relation to the Council's Policy. The Council's requirements in relation to auto-forwarding are not always being adhered to which increases the risk of sensitive data leaving the Council network.	The Council should ensure that the use of auto-forwarding rules is addressed as part of information security related communications and training to staff.	**Medium**	**Response:** Accepted Auto forwarding of emails externally has been disabled since March 2019. **Officer Responsible for Implementation:** N/A – complete **Timescale for Implementation:** 30 April 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – Email Auto-Forwarding Arrangements

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Exchange Online has been configured to prevent end users from setting up rules which would result in data leaving the Council network.				
2	There are currently no technical controls in place to prohibit the creation of externally facing auto-forwarding rules. Since the migration to Exchange Online, the CGI Messaging team receive alerts which prompt them to remove externally facing rules as they are set up, however, staff still have the ability to create these rules. As noted in action 1 above however, we identified 192 externally facing rules in use by 97 different users. We were advised by the Messaging team that these were legacy rules that had been set up prior to the migration to Exchange Online and therefore had not generated alerts. Moreover, through sample testing we identified one instance where the rule in place resulted in Council data leaving the Council's network. This related to a procurement project and we have since confirmed that the rule has been removed, and that the data has been deleted.	The Head of Information and Data Protection Officer should liaise with the CGI Messaging team so that additional technical controls can be implemented, to prevent externally facing auto-forwarding rules being set up. Action should also be taken to ensure that all existing externally facing rules are removed. Thereafter the Messaging team should be requested to conduct period checks, to verify that the controls are operating effectively and that no externally facing rules have been created. The Council should also consider whether to implement a formal exception process, where there is a legitimate business reason for the creation of external auto-forwarding rules.	**High**	**Response:** Auto forwarding of emails externally has been disabled since March 2019. Therefore, there is no need to undertake periodic checks. In respect of a formal exceptions process, this will be developed with the Information Security Board. **Officer Responsible for Implementation:** Head of Information and Data Protection Officer **Timescale for Implementation:** 30 April 2019 for formal exceptions process.

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – Email Auto-Forwarding Arrangements

No.	Observation and Risk	Recommendation	Priority	Management Response
3	Some of the key Council distribution lists are configured in such a way that only relevant staff can interact with them. This ensures that emails cannot be forwarded from these lists in error (e.g. via the reply all function or an incorrectly created auto-forwarding rule). Not all distribution lists are configured in this way and the Messaging Team advised that they act on direction from the Council in this respect. However there may be scope to apply similar configurations to other distribution lists. Furthermore, Exchange Online has additional alerting capability through its Security and Compliance module. As such it may be possible to further enhance the controls around distribution lists, thereby minimising the risk of auto-forwarding rules being created to send to multiple parties. There is currently an increased risk that emails containing personal data could be auto-forwarded to distribution lists in error.	Council management should consider reviewing the distribution lists currently in use and, using a risk based approach, determine whether any higher-volume lists should be restricted to specific individuals. The Head of Information and Data Protection Officer should liaise with CGI to determine whether alerts can be implemented to identify rules which have been created to send internally to distribution lists. The Council should also consider whether rules created to send to distribution lists should be managed via a formal exception process, where there is a legitimate business reason for this.	**Low**	**Response:** Distribution lists have been reviewed and a number have been disabled to be reviewed again in 3 months. Further restrictions on higher-volume lists will be considered through the Security Working Group (SWG). The use of alerts and a formal exceptions process will also be managed through the SWG. **Officer Responsible for Implementation:** Head of Information and Data Protection Officer **Timescale for Implementation:** 31 August 2019