Item 3(b)

15th January 2020

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

1. Introduction

1.1 As part of the agreed Internal Audit plan we have carried out a review of the fundamental controls that have been applied to the Council's IT systems, through an audit of IT General Controls.

1.2 The Corporate and Education schools domain are separate networks, which allows different controls and processes to be in place aligned to the needs and risk profile of the users. The purpose of the audit was to obtain assurance that there are a broad range of IT controls in place on the Education network and that these are operating as designed to ensure the effective overall management of the IT environment.

1.3 The scope of the audit focused on the schools domain and included a review of:

- The structure and organisation of the IT function;
- Hardware and Software asset management;
- The security control framework;
- The IT Strategy, and
- Change control.

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 eight recommendations which management should address.

3. Main Findings

3.1 The Council has a suite of policies and guidance in place for the Council family which outlines the Council's requirements in relation to information security and the use of IT. However the Information Security Policy that is published on Glasgow Online (the primary intranet resource for school based staff) does not reflect the Council family policy and is out of date.

3.2 We found that the password policy settings in place within the schools domain do not fully align to the Council family guidelines.

3.3 The Software Asset Register relating to software installed on the schools domain is out of date and is not adequately maintained. It should be noted that schools (with the exception of secondary schools) can purchase and install software locally and there is a requirement, under Management Circular 59, for software licensing terms to be complied with at an establishment level. A review of software licensing compliance within educational establishments will be undertaken in a future audit.

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

3.4 From review of the accounts on Active Directory (AD - The Council's network authentication service[1]) we identified a number of generic accounts (e.g. guest accounts) in place across school establishments, including some with a password set to never expire. Active accounts were also found which related to staff who had left the organisation.

3.5 A review of both domain and local admin rights was carried out and found that the domain admin rights could be further restricted. There are also a portion of pupils (i.e. those based at Additional Support for Learning – ASL – establishments) who have local admin rights and could therefore install potentially harmful software onto devices. The allocation of local admin rights to ASL based pupils was for operational purposes however this is now under review. Steps have been taken to remove access in one ASL establishment, since the audit fieldwork was completed, and the business implications are being assessed to determine whether this can be applied across all ASL establishments.

3.6 There are no technical controls in place to restrict the use of removable media, particularly unencrypted USB sticks which are known to be in use on the education schools domain. This was found in a previous 2018/19 audit of establishments and work is ongoing to remediate this, and as a result no further recommendation has been made.

3.7 An action plan is provided at section four outlining our observations, risks and recommendations. We have made eight recommendations. 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.	3
Medium	Less critically important controls absent, not being operated as designed or could be improved.	4
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

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

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

3.10 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.

[1] Active Directory network authentication is the way in which the Council controls access to the network by users (eg initial username and password control to log onto the network)

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Roles and responsibilities have been clearly defined, documented and understood by staff.				
1	From a review of the Glasgow Online intranet, for Education Services staff, we found an outdated version of the Council family's Information Security Policy. The version currently displayed refers to the Council's previous IT provider and superseded data protection legislation. Glasgow online is the primary reference point for teachers and establishment based staff and, as a result, there is currently an increased risk that staff may be unaware of the Council's requirements in relation to information security, and their responsibilities in line with these.	Education Services should ensure that Glasgow Online is updated to reflect the current Information Security Policy and associated guidance. Education Services should also ensure that Glasgow Online is kept up to date when new versions are published.	**Medium**	**Response:** A link to the Information Security policy on Connect will be added to Glasgow Online as opposed to a copy of the policy. This will ensure that users are directed to the most up-to-date version. **Officer Responsible for Implementation:** Education ICT Business Partner **Timescale for Implementation:** 31 December 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: A Software Asset Register is maintained and compliance with software licensing terms is recorded and monitored.				
2	The Software Asset Register for the schools domain is not currently being kept up to date by CGI, although this is a requirement of the IT contract. In addition, the software licensing agreements have not been included in the Register for all software instances that CGI are responsible for. As a result there is an increased risk that CGI may not be able to demonstrate compliance with all software instances.	The Strategic Innovation and Technology (SIT) team should liaise with CGI to request that the Software Asset Register, relating to the schools domain, is brought up to date for software managed by CGI. Thereafter this should be maintained on an ongoing basis to demonstrate compliance with software licensing terms.	**Medium**	**Response:** Accepted. SIT has requested the Register be updated and maintained. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 December 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Users authenticate using unique user names and strong passwords.				
3	We obtained a copy of the password policy settings in place for the schools domain and found that these could be strengthened. The policy settings apply to both staff and pupils across the schools domain. As such this covers all pupil age ranges and a variety of educational needs. Functionality is now available, however, to specify multiple password policies within a single domain. The appropriateness of the Council's password policy is reviewed regularly to ensure alignment with the relevant standards (e.g. Payment Card Industry Data Security Standards – PCIDSS) and the adoption of best practice, where possible (e.g. National Cyber Security Centre – NCSC – guidance). This was noted in the recent Corporate User Access and IT Permissions audit. The current password settings increases the risk of unauthorised system access.	The SIT team should liaise with CGI so that age/role based password settings are applied, which are suitable for both staff and pupils.	**High**	**Response:** Accepted. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 March 2020

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Users authenticate using unique user names and strong passwords.				
4	From a review of the accounts on AD we found that the privileged user accounts (domain administrator permissions) could be reviewed and further restricted. Periodic reviews take place by CGI, however we also found that a leaver's account was active within this permission group, suggesting that this element of the control framework is not operating effectively. This increases the risk of unauthorised or inappropriate access to systems.	The SIT team should liaise with CGI to ensure that a review of the privileged user accounts in AD is carried out with a view to enforcing a least-privilege administrative permission model. SIT should also liaise with CGI to request that they investigate why the leaver was not identified as part of the privileged account review, and ensure that steps are taken to correct this control failure going forward.	**High**	**Response:** Accepted. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 December 2019
5	From a review of the accounts on Active Directory we found that there were a number of generic accounts (e.g. guest accounts) created across a number of the establishments. In total there are 56 active guest accounts of which 31 have the password set to never expire, and in some cases had not been updated in a number of years. The observation increases the risk of unauthorised or inappropriate access to systems.	(a) The SIT team should liaise with Education Services and CGI to ensure that a review of the generic accounts in AD is carried out and reduce these where possible. (b) Where there is a valid business reason for retaining generic accounts, Education Services should ensure that appropriate controls are put in place for the management of these, ensuring that: • Accounts are assigned to a named owner. • Account access is tracked and monitored. • Accounts are cleansed after use. • Passwords are regularly updated in line with the Council's requirements.	**High**	**Response:** Accepted. **Officer Responsible for Implementation:** **(**a) Head of Information and Data Protection Officer (b) Education ICT Business Partner **Timescale for Implementation:** 31 March 2020

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Account permissions are assigned on the basis of least privilege and are removed timeously when no longer required.				
6	Both staff and pupils within Additional Support for Learning (ASL) schools have been assigned local admin rights, which allows them to install software locally on devices. This is a historic arrangement to enable specialist software, used within ASL schools, to operate. However an incident occurred recently at one school, whereby a pupil misused the admin rights granted, and the appropriateness of this arrangement is now being questioned. Admin rights have been removed from pupils at the school and the impact of this is being assessed. More widely, the phased removal of pupil admin rights is being implemented across ASL schools to determine if this can be applied across all ASL establishments. The current arrangement however increases the risk that pupil admin rights continue to be misused, resulting in malicious software being installed.	EDS, with assistance from CGI, should ensure that the pupil admin rights review in ASL establishments is concluded and that elevated rights are removed.	**Medium**	**Response:** Accepted. This review is ongoing and privileges have been removed from a number of ASL establishments. **Officer Responsible for Implementation:** Education ICT Business Partner **Timescale for Implementation:** 28 February 2020

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Account permissions are assigned on the basis of least privilege and are removed timeously when no longer required.				
7	From an HR leavers report we selected a sample of 10 staff for further review. From this we found that: • Leavers documentation had only been submitted in 3 (30%) of cases and the accounts were disabled. • A further 5 (50%) accounts had been disabled through the use of automated process (scripts). • 2 accounts (20%) remained active. The leavers process is currently under review and an action plan is being devised which is aimed at increasing compliance with the process. In order to compensate an automated script was run in March 2019 to identify and remove users who had not logged on for a prolonged period of time. This however is not undertaken on a regular basis, whereas a 35 day process exists on the corporate domain. There is therefore an increased risk that accounts remain active for longer than required.	The SIT team should liaise with Education Services, and with CGI, to ensure that a formal process can be implemented on the schools domain to disable inactive accounts on a routine basis.	**Medium**	**Response:** Accepted. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 December 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Schools Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Complete and accurate audit trails are in place.				
8	Security event logging is in the process of being rolled out across both the corporate and schools domain and we have been advised that the events monitored align to a protective monitoring standard. Event logs will be monitored via the Security Operations Centre (SOC), which will identify events that warrant further investigation. Although events have been aligned to the protective monitoring standard, the contract with CGI requires vendor best practice to be adopted. As a result there may be opportunities to further enhance the security monitoring being undertaken. We also noted that the events being monitored across both the schools and corporate domains differ, with reduced logging on the former, although we were advised that both align to the protective monitoring standard. As a result there is a risk that security monitoring is not being undertaken as fully or as consistently as possible, and key events may not be identified.	The SIT team should liaise with CGI to review the logging in place within AD and consider whether the adoption of additional logging would enhance the security of the systems. Moreover, the logs in place across both domains should be reviewed and applied consistently.	**Low**	**Response:** Accepted. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 March 2020