Item 3(a)

15th January 2020

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Corporate Review – IT General Controls – Corporate 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 in the Corporate Domain and that these are operating as designed to ensure the effective overall management of the IT environment.

1.3 The scope of the audit included:

- The structure and organisation of the IT function.
- Software asset management.
- The security control framework.
- IT disaster recovery arrangements.
- IT governance, including roles and responsibilities, change control and authorisation arrangements.

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 four recommendations which management should address.

3. Main Findings

3.1 A number of key controls are in place and generally operating effectively. The Council has a suite of policies and guidance in place for the Council family to ensure that staff are aware of their responsibilities in relation to information security. A control framework is in place to manage system changes and implementations.

3.2 Software patching and anti-virus controls are in place, with compliance reported via the Security Working Group and Information Security Boards. Network security monitoring is in the process of being enhanced further through the implementation of the Security Operations Centre (SOC), which will strengthen the Council's current IT security arrangements. We are advised that this will be fully in place by the end of January 2020.

3.3 However we also identified a number of areas where key

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

controls require to be further strengthened. There are controls in place to ensure that USB ports are suitably restricted, however once a peripheral device has been unblocked ("whitelisted") it retains that status indefinitely. Reviews are currently not undertaken to ensure that there is still a requirement for this. We also found that Hard Disc Drives (HDDs), which are also portable and tend to have greater capacity, are not required to be encrypted prior to being whitelisted.

3.4 The audit confirmed that, although a Service Restoration plan is in place, this is currently in draft and may no longer reflect the Council's DR environment. Management have advised there is ongoing work to review the business requirements outlined in the Business Continuity Plans (BCPs) of Services, which will inform this.

3.5 We also found that there is currently no DR testing plan in place and no testing has been carried out since the IT contract with CGI went live in April 2018. This is built into the contractual obligations but is currently not being met.

3.6 An action plan is provided at section four outlining our observations, risks and recommendations. We have made four 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.	1
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

3.8 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.

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

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

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: The use of removable media is blocked by default.				
1	We reviewed the security controls in place around the use of removable media and found that, once whitelisted[1], USB devices are not subject to review to ensure they are still required. Furthermore Hard Disk Drives (HDDs), which have a larger capacity than USB sticks, are not required to be encrypted in order to be whitelisted. We found instances of these in use by Apple device users, within the Council’s Graphics Team. These are not hardware encrypted products although we were advised that Apple software is used to encrypt the external HDDs. This however is not actively managed by CGI. Without the appropriate controls in place for the management of electronic data there is an increased risk that the Council may not be able to fulfil its data protection obligations.	The Strategic Innovation and Technology (SIT) team should liaise with CGI to facilitate a review of the unblocked removable media currently whitelisted on the estate. Devices which are not in use, or no longer have a valid business reason for being used, should be removed. Furthermore controls around HDDs should be enhanced to ensure that the same level of protection is put in place for these devices, as with USB memory sticks.	**High**	**Response:** The whitelist will be reviewed. However, upon completion of the End User Compute programme, expected by the end of 2020, this will be fully replaced. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 March 2020

[1] “Whitelisting” refers to removable devices (USB storage pens and storage drives, cameras etc) that are automatically blocked from networked computers. Whitelisting effectively allows a specific device to be used by-exception through an authorisation process.

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

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

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Contractual obligations in relation to disaster recovery are met, reviewed and updated.				
2	The Council has defined its business continuity requirements and discussions are ongoing with CGI to agree the level of DR provision required to support these. An overarching draft Service Restoration (DR) plan, dated March 2018, was provided however it is unclear whether this requires updating, following the relocation of data centres during 2019. More widely we found that only CareFirst was supported by an application specific DR plan. Some additional assurance in relation to DR was obtained however. Regular backups are taken and we have been advised by, the Service Director at CGI, via the Head of Technology, that additional server capacity has been made available offsite for the restoration of services, should a DR event occur. However without finalised plans there is currently an increased risk that systems may not be recovered in a timely manner or at all.	The SIT team should ensure that the overarching Service Restoration plan is reviewed and updated, by CGI, as necessary. This should be finalised and approved, by the Council thereafter. At an application level DR plans should be developed by CGI, and approved by the Council, for the Council's key applications. These need to be comprehensive in terms of roles and responsibilities, and reflect the assumptions and priorities set out in Council Business Continuity Plans.	**High**	**Response:** Accepted **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** 31 January 2020

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

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

No.	Observation and Risk	Recommendation	Priority	Management Response
3	From a review of Schedule 8.6 of the service contract with CGI, relating to DR testing, it was noted in that: • CGI should undertake DR testing at least once every 2 years • CGI should provide the Council with an annual plan of DR related activity (including testing). However, there is no test plan in place and no testing been carried out since the start of the contract in April 2018. As a result there is an increased risk that in the event of a disaster, systems may not be restored as expected, impacting the Council's ability to deliver key services.	The SIT team should ensure that contractual requirements outlined in schedule 8.6 are being met. Where these are not being met appropriate action should be taken to escalate issues via the appropriate contract management channels.	**High**	**Response:** Accepted. Discussions are ongoing in relation to the DR test plan. **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 – Corporate Domain

No.	Observation and Risk	Recommendation	Priority	Management Response
4	A controlled DR exercise was conducted for the SAP platform, by the previous IT provider, ACCESS. This resulted in a lessons learned exercise being undertaken and an action plan being created. No evidence could be provided to show that the action plan from the lessons learned exercise has been progressed or that the improvement actions have been implemented. As a result there is currently an increased risk that key areas of improvement are not being addressed in relation to SAP DR.	(a) The SIT team should review the action plan and where possible seek to implement the improvements set out. (b) For future DR test lessons learned exercises, roles and responsibilities should be clearly identified to ensure actions are progressed in a timely manner. Ongoing actions should be reported to the appropriate ICT Board.	**Medium**	**Response:** Accepted. **Officer Responsible for Implementation:** Head of Technology **Timescale for Implementation:** (a) Complete. The ACCESS lessons learned plan has been reviewed. (b) As per recommendation 3 above, testing plans will be obtained from CGI by 31 March 2020, with testing carried out thereafter. Future lessons learned exercises for DR tests will present action owners clearly and these will be reported to the appropriate ICT Board.