GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

1.   Introduction

1.1   As part of the agreed Internal Audit plan we have carried out a review of the Mimsy application used by Glasgow Life to catalogue the Council's civic collection. The system records the history of each of the collection items and for the most part this is limited to non-sensitive data (e.g. the catalogue number, location and condition of the item). However there are some instances where personal data (e.g. name and address details of previous item owners) and commercially sensitive data (e.g. valuation and information relating loans) are recorded also. The system provider is Axiell, and the contract with the vendor is managed by CGI on behalf of Glasgow Life.

1.2   The purpose of the audit is to gain assurance that the application controls are operating as designed and are effective in preventing and detecting weaknesses that could adversely impact on the control of collection items within the Mimsy application. The scope of the audit included:

- Software licensing arrangements;
- Documentation in relation to the Mimsy application, and staff training and awareness in relation to these procedures;
- User access and permissions management;
- Software updates and security patching;
- Inputs and outputs to/from the application;
- Error and exception reports, where relevant;
- Audit trails;
- Data storage arrangements and back up processes; and
- Business continuity planning and disaster recovery.

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   We found that there is adequate documentation and training in place for the administration and use of the system. Access to Mimsy is only granted to users who have completed the new user training provided by a long term user and system administrator. The system administrator role itself is suitably restricted to two managers. Inputs to the system (e.g. new acquisitions or the relocation of collection items) are suitably approved and checked for accuracy as part of the input process.

3.2   However we did identify some control deficiencies. The software licensing arrangements in place are currently unclear. We were unable to obtain licence documentation to confirm the licensing and support agreement (and any

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

limitations) in place. System support however was utilised during the audit fieldwork, thereby providing some assurance in this area.

3.3 The audit trail for requesting and approving system access was not complete in all cases; access has historically been arranged by email with managers but in some cases has been arranged verbally. We were advised that system accounts are reviewed by the system administrators, however upon further review we found that this is not carried out on a regular basis. Account reviews are limited to verifying that the user exists and do not currently include a review of the permissions assigned, and their suitability to the role carried out.

3.4 Users are assigned unique usernames, however, the passwords settings could be strengthened.

3.5 The server is located onsite at the Glasgow Museum Resource Centre (GMRC) and access to the server room is controlled via card entry system. However we found that access was not limited to staff who require access as part of their role.

3.6 We found that, although there is a high level, organisational Business Continuity Plan (BCP) in place for Glasgow Life, a business interruption as a result of Mimsy being unavailable was not specifically addressed. Disaster Recovery (DR) for the Mimsy system is limited to restoration from back up files. We were able to verify that back-ups of the system are taken on a regular basis, thereby minimising the potential for data loss, however these are not tested. In addition we were unable to confirm whether action is taken in response to files which fail to back-up correctly. There is therefore a risk that the Mimsy application could be unavailable for a significant period of time, depending on the scenario. In the absence of specific business continuity arrangements, Glasgow Life may therefore be unable to provide the public with access to the Council's civic collection.

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

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

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

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: Glasgow Life – Mimsy Application Review

4. Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Access to the system is restricted to authorised staff.				
	We found that the password policy in place for the Mimsy system requires to be strengthened and aligned to the Council Family's password policy. The Council family's password guidance requires users to utilise strong, (at least) nine character passwords, which should be updated on a regular basis. As such there is an increased risk of unauthorised access to the Mimsy system.	Glasgow Life should ensure the password policy settings for Mimsy are strengthened and aligned to the Council family's password guidance. In doing so, Glasgow Life should ensure that password complexity is enabled, where the system allows this.	**High**	**Response:** Glasgow Life promote the use of strong passwords in line with the Council family's guidance however it can only be enforced when the systems software can set it as mandatory. MIMSY is only accessible via Glasgow Life networked PCs therefore users require a Glasgow Life Active Directory login which meets the required password complexity before they can access the application. We will ensure that the password arrangements are strengthened. **Officer Responsible for Implementation:** Glasgow Life Head of Transition **Timescale for Implementation:** 31 March 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
2	We confirmed that a review of user accounts was being carried out while we were conducting the audit, however we noted that such reviews are not carried out on a regular basis. The administrator advised that they intend to conduct reviews on a 6-monthly basis going forward. Without a regular review of user access there is an increased risk that accounts remain active when they are no longer required.	Glasgow Life should formalise and document the account review process ensuring that reviews are conducted on a regular basis.	**High**	**Response:** Glasgow Life have introduced a 6 monthly systems audit process where the system administrator completes a checklist and resolves emerging issues. **Officer Responsible for Implementation:** Glasgow Life Head of Transition **Timescale for Implementation:** 31 March 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
3	We found that a complete audit trail was not always available in order to demonstrate that system access had been granted following an approved management request. Access is usually arranged by email but is also occasionally organised verbally by phone, thereby further reducing the effectiveness of the audit trail. The administrator currently assigns user access permissions based on their knowledge of the staff member and their role, however this is not formally requested as part of the user access request. Without a complete audit trail in place it is not possible to easily determine if the rights assigned to users are appropriate.	Glasgow Life should ensure that a formal user access process is put in place the management of system access requests. As part of this the administrator should ensure that user permissions are clearly outlined in the request and that suitable arrangements are put in place for the retention of user access documentation.	**Medium**	**Response:** Requests for access or changes to the level of access will be in writing from a manager. The request for access to the Mimsy server will be completed by the user and sent to CGI by the systems administrator. Acceptable use conditions will also be signed and all requests will be filed. **Officer Responsible for Implementation:** Collections and Access Manager **Timescale for Implementation:** 31 March 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
4	During the audit it was found that a declaration form was in draft and had been used in some but not all instances as part of the user access request process. This outlines Glasgow Life's expectations of users in relation to password management and copyright arrangements and should be signed by all new users. There is therefore an increased risk that not all staff with system access have been advised of, and have confirmed their adherence to, these key points.	Glasgow Life should finalise the declaration form and ensure that this is formally included in the user access process going forward. A review should also be carried out to ensure that all current users who have not completed the declaration, do so.	**Low**	**Response:** A declaration will be issued to all new users and retrospectively completed by existing users. **Officer Responsible for Implementation:** Collections and Access Manager **Timescale for Implementation:** 30 April 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
5	The server room is located onsite at the Glasgow Museum Resource Centre (GMRC). Access to the room is controlled by a secure card entry system. However, upon investigation it was found that 327 staff had access to the room as it had previously been used for other purposes. In addition to the information security risk of uncontrolled access to servers, there is an increased risk that servers could be vandalised or accidentally damaged, resulting in a loss of system access/data.	Glasgow Life should review the number of staff who have access to the server room ensuring that access is minimised as far as possible.	**Medium**	**Response:** Server room access rights will be restricted to essential users only. **Officer Responsible for Implementation:** Logistics Programming Manager **Timescale for Implementation:** 31 March 2019

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Business continuity and disaster recovery plans have been developed and are maintained.				
6	There is currently no formal Business Continuity Plan (BCP) or Disaster Recovery (DR) plan in place for the Mimsy system. Should an issue occur, we were informed that Mimsy would be restored from back-up, which could have an impact on the Recovery Time Objective (RTO – the amount of time that the function can reasonably operate without the system, before it has a critical impact) and may result in some data loss. We confirmed that CGI carry out full and incremental back-ups of the system to minimise the amount of data that would be lost, if there was a requirement to restore the system from back-up. However we found that the back-ups are not tested to ensure that they are not corrupt and could be used to successfully restore system data if required. Furthermore we noted errors in the back-up reports and were unable to determine what action is taken to remediate these. In addition to the back-ups taken by CGI, the administrator takes a nightly back-up of the system data and saves this to an encrypted hard drive, which they take home each night. Similarly, this back-up	Management at the GMRC should review their Business Continuity requirements and ensure that an appropriate plan is put in place which addresses a loss of IT, including Mimsy. In addition, the Glasgow Life business partner should obtain assurance from CGI that the back-ups taken from the Mimsy system would allow the system to be restored, as fully as possible and in accordance with the RTO, in the event of an IT disruption. Once adequate assurance has been obtained management should review the appropriateness of the additional back-ups taken by the administrator and determine whether these are still required. If so, a more appropriate offsite storage arrangement should be put in place.	**High**	**Response:** Glasgow Life will seek advice from the SIT BCP and DR resources and the CGI Applications team. **Officer Responsible for Implementation:** Glasgow Life Head of Transition **Timescale for Implementation:** SIT / CGI Engagement: 31 May 2019

Title of the Audit: Glasgow Life – Mimsy Application Review

	is also not tested. There is therefore an increased risk that the current arrangements in place for the recovery of Mimsy would not be successful should an incident occur.			

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Personal and sensitive data is accurately recorded in controlled fields to ensure that it is suitably restricted, where necessary.				
7	Donor information, including the address provided at the time of acquisition, is recorded within Mimsy. However it was found that, of the 26,000 contact records, over 17,500 addresses were not recorded in the correct field and are therefore viewable to most system users (Volunteer users do not currently have these permissions). As such, basic personal data which would otherwise be restricted through user access permissions is currently accessible to users with minimal privileges.	Glasgow Life should liaise with the Mimsy system provider to determine whether the addresses held in incorrect fields can be relocated to the correct, suitably controlled, field.	**Medium**	**Response:** We will initiate a request to CGI, who manage the Axiell contract on behalf of Glasgow Life, to determine the feasibility of having donor addresses relocated to the contacts table within the database. The contacts table is only accessible to staff that need to see this data. **Officer Responsible for Implementation:** Collections and Access Manager **Timescale for Implementation:** 31 March 2019.

GLASGOW CITY COUNCIL INTERNAL AUDIT SECTION

COMMITTEE SUMMARY

Title of the Audit: Glasgow Life – Mimsy Application Review

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: There are adequate licensing and support arrangements in place for the system				
8	The software licensing arrangements in place for the Mimsy system are currently unclear. We were unable to obtain sight of the software licence agreement or invoice that would outline the type of licence in place and any limitations on use that apply. The administrator advised that they believed that a site licence was in place for the use of Mimsy, however, we found that there were a total of 197 users listed across multiple sites. Clarity over the definition of 'site' is therefore essential in order to determine whether Glasgow Life are compliant with the terms and conditions. As such there is an increased risk that the system is being used outwith the agreed terms of use.	The Glasgow Life business partner, should liaise with the CGI Software Asset Management team to clarify the terms of the licence and confirm whether these are being complied with. If it is found that Glasgow Life is not complying with the terms of the licence steps should be taken to address this.	**Medium**	**Response:** CGI advised that a Site Licence means 'anyone working in a contracting organisation can use it'. Axiell confirmed that the site licence covers the current usage pattern of the MIMSY system within Glasgow Life. **Officer Responsible for Implementation:** Glasgow Life Head of Transition **Timescale for Implementation:** 31 March 2019