Loch Lomond & The Trossachs National Park Authority

Review of GIS Application

Final Report

AUDIT GLASGOW

May 2022

Glasgow CITY COUNCIL

Loch Lomond & The Trossachs National Park Authority
Review of GIS Application

Table of Contents

Loch Lomond & Trossachs National Park Authority
Review of GIS Application

1. Introduction

1.1 As part of the agreed Internal Audit plan we have carried out a review of the Geographic Information System (GIS) Application (ARCGIS) within Loch Lomond & The Trossachs National Park Authority (the Park Authority).

1.2 The Park Authority protects and preserves the natural and cultural heritage of the Park encompassing around 720 sq miles (1,865 sq km) across a range of terrains, including mountains, lochs, and rivers. The Park Authority uses GIS software (provided by Esri) on a shared service basis with the Cairngorms National Park Authority to visualise, analyse and understand the vast spaces that make up the National Park. Access to the system is controlled by the GIS team based in Balloch and although most data is unrestricted, some exceptions exist. The ARCGIS application has several components accessible via desktop, tablet and smartphone.

1.3 The purpose of the audit was 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 operation of the ARCGIS application.

The scope of the audit included an assessment of:

- Software licensing arrangements,
- System manuals and user guides, including staff training and awareness,
- Back up processes,
- 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,
- Business continuity planning / disaster recovery arrangements.

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 some key controls are in place and operating effectively. The system licence for the ARCGIS server-based application is included in the licence inventory and the number of users was confirmed as being within the licence parameters. There are two system administrators and there is a detailed administrator guide and availability of training to all users. The location of the server and security arrangements described to us were reasonable, although this was not verified in person by the auditor. Links to various guides available through the ARCGIS Portal were provided which indicated a wealth of information / technical support for operating the system. These are accessible to anyone using the publicly available Portal.

3.2 Data input to the ARCGIS application was found to reasonable, with input controlled through the permissions granted to users. System data is backed up at regular

intervals to minimise the risk of data loss and backups are held off-site with suitable restricted access.

3.3 System users are only granted access to the system following the completion of a new start form. For a sample of five users identified from the user list we confirmed via Human Resources that all were current employees of the Park Authority. Similarly, we selected a sample of 5 leavers and verified in all instances that system access had been revoked timeously after their leaving date.

3.4 Patches and upgrades are applied to the internally hosted systems, including the ARCGIS application, and these are recorded on a change control file. Application support and maintenance services are in place and these are received from the software provider, Esri. The ARCGIS server is nearing end of life, however we were advised that a plan is in place for its upgrade, and this is expected to be completed by October 2022.

3.5 In relation to error and exception reporting, server logs are reviewed daily and scheduled system checks of all ARCGIS related applications are undertaken, with processes in place to investigate and resolve any issues identified. Although no proactive sample checking of system use takes place, some control over inappropriate use is exercised by the GIS team, through data-viewing and user roles permissions, patrolling of log-in activity as well as controlling of published information.

3.6 The system generally holds mapping data however there are some occasions where the information gathered can be sensitive in nature (e.g. information relating to protected species or individuals who have been sanctioned by the Park Authority). Where this is the case this information is stored in a restricted area accessible only by the GIS team. The Park Authority's document retention schedule includes entries relating to the ARCGIS application and the stated period of seven years should be sufficiently lengthy. There is a Park Authority statement on destruction arrangements for paper records of which a copy was obtained and the key arrangements noted. Most information is shared through the ARCGIS portal, the publicly available browser. However, within the GIS team, there is restricted folder access for any information obtained from other organisations. There are also joint working / agreements in place where information is shared with third parties.

3.7 However, our audit testing found that there are areas of non-compliance. Generic user accounts are routinely used, some of which have edit rights, and access is shared by groups of users e.g. Ranger team members. Although we were advised that this is necessary for operational requirements this reduces the level of accountability within the system.

3.8 Moreover, the ARCGIS portal does not enforce periodic password changes and Ranger Teams' credentials are only reset at the end of the season. In general the password security requirements could be further enhanced.

3.9 The various outputs which can be generated from ARCGIS were documented and examples provided. However, although an organisational activity report includes a date / time stamp for entries this is limited and does not record all transactions. There is also no storing / archiving of the organisational activity reports.

3.10 The Park Authority has a detailed Business Continuity Plan (BCP) in place which includes the arrangements in place for ICT Disaster Recovery (DR), data back-up / restoration and alternative accommodation. We noted however that although

there are plans to conduct DR testing as part of a process of moving to Cloud later in 2022, there has been no BCP / DR testing carried out for several years. This has been highlighted as part of the 2021/22 Business Continuity Planning audit and a high priority recommendation was made as part of that review, hence no further recommendation for BCP testing has been made as part of this review. We noted however that back up testing is not routinely undertaken.

3.11 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
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

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

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

3.14 It is recommended that the Chief Internal Auditor submits a further report to the Audit and Risk Committee on the implementation of the actions contained in the attached Action Plan.

4. Action Plan

Title of the Audit: Loch Lomond & The Trossachs National Park Authority – Review of GIS Application

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: User Access control including the use of unique passwords, changing passwords and use of strong passwords is exercised.				
1	User account management arrangements could be further enhanced. Generic user accounts are routinely used within the Parks Authority and user credentials are shared between groups of multiple staff. A review of the account permissions found that some of these accounts had edits rights and are capable of changing data within the system. Furthermore, the ARCGIS Portal does not request periodic password changes and Ranger Team passwords are only reset at the end of the season. A list of user accounts and passwords is also held centrally by the GIS Manager. The current password policy could be also be strengthened through the inclusion of special characters and, although the system can be accessed remotely, two-factor (2FA) / multi-factor authentication (MFA) is not currently in use to validate remote users (although a Virtual Private Network (VPN) is in use).	The GIS manager should review the user access arrangements in place and determine whether it is possible to utilise named accounts to improve the levels of accountability within the system. Furthermore password security arrangements should be strengthened to ensure that: • users are required to change their password on a periodic basis; • the password rules in place are further enhanced, where the system allows (e.g. through the implementation of password complexity or 2FA / MFA). • a central list of accounts and passwords is not held.	**High**	**Response:** Accepted. To use generic & shared logins we need to control the passwords in use and the GIS team need to be able to set and manage passwords. Access to this list is restricted and users only know the logins assigned to them. We can increase the complexity of the passwords being assigned to users. We will implement the use of MFA for administrators and users with management access. **Officer Responsible for Implementation:** GIS Manager **Timescale for Implementation:** 31 October 2022

No.	Observation and Risk	Recommendation	Priority	Management Response
	The current arrangements increase the risk of unauthorised access to the ARCGIS system.			

Title of the Audit: Loch Lomond & The Trossachs National Park Authority – Review of GIS Application

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: A satisfactory audit / management trail recording additions, amendments and deletions to the system is maintained.				
2	The organisational activity report currently provides a limited audit trail of system updates, although it was noted by the GIS Manager that this is sufficient for current use. We were advised that the report parameters can be amended to record a more detailed transaction history, however this may be excessive and could result in capacity issues. Nonetheless, there may be value in having additional logs to compensate for the reduced accountability arising from the use of shared accounts. Logs could include anomalous logins, access to sensitive information, use of admin / high powered accounts etc. Moreover, organisational activity reports are only run on an ad hoc basis and as such there is no proactive monitoring or archiving of these reports. There is therefore currently an increased risk that system misuse is not detected and investigated.	The GIS manager should review the current audit trail reporting parameters and assess the feasibility of updating these so that they include a more detailed transaction history. In doing so the manager should consider the risk of not capturing all updates alongside any limitations that may exist, e.g. storage capacity, monitoring resources etc. Thereafter logs should be suitably stored and archived as necessary.	**Low**	**Response:** Accepted. We will investigate the feasibility of adding full transaction history for any data that warrants this level of control. For system changes we can look at what is available and if we need to export and save any activity logs, or just increase the frequency and nature of checks. For shared user accounts, we will look to enable authentication logs to identify any anomalous login behaviour and/or data access **Officer Responsible for Implementation:** GIS Manager **Timescale for Implementation:** 30 September 2022

Title of the Audit: Loch Lomond & The Trossachs National Park Authority – Review of GIS Application

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Back Ups are taken at regular intervals and are routinely tested.				
3	We found that backups are taken at regular intervals, with daily incremental backups and a weekly full backup of the system taken, to reduce the risk of data loss. We noted however that although this is the case these are not routinely tested to assess whether these can be restored. Without regular testing there is an increased risk that data cannot be restored effectively when required.	Management should ensure that periodic backup testing is undertaken to routinely verify that data can be restored.	**Medium**	**Response:** Accepted. There are two levels to consider; 1. Data and information (GIS team responsible for checking their backup/restore); 2. Systems (including data) – ICT manage server backups and DR. **Officer Responsible for Implementation:** 1. GIS Systems Officer 2. IS Manager **Timescale for Implementation:** 1. 31 December 2022 2. 31 March 2023