Loch Lomond & Trossachs National Park Authority

IT General Controls

Final Report

AUDIT GLASGOW

Date

April 2021

Glasgow CITY COUNCIL

Loch Lomond & Trossachs National Park Authority
IT General Controls

Table of Contents

Loch Lomond & Trossachs National Park Authority
IT General Controls

1. Introduction

1.1 As part of the agreed Internal Audit plan we have carried out a review of the effectiveness of the IT General Controls in place at Loch Lomond & Trossachs National Park.

1.2 IT General Controls (ITGC) are the fundamental controls that can be applied to IT systems such as applications, operating systems, databases, and supporting IT infrastructure. The objectives of ITGCs are to ensure the integrity of the data and processes that the systems support.

1.3 The scope of the audit included a review of the following aspects:

- IT strategy and governance.
- IT asset management controls.
- The security control framework, including user access management, device control, patch management and security monitoring.
- Change management.
- 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 five recommendations which management should address.

3. Main Findings

3.1 A number of the key controls are in place and are operating effectively. We found that a Service Level Agreement (SLA) is in place for network connectivity with appropriate performance monitoring in place. A suitable monitoring process for progress made on IT areas of work is in place.

3.2 An IT asset register is in place and there is a process to ensure it is regularly updated. The organisations Information Security Policy has received senior management approval and has been communicated to staff.

3.3 The use of admin accounts is restricted to appropriate individuals and the guest account is disabled. There are controls in place to prevent the use of removable media such as USB drives. We found that appropriate patch management controls are in place to ensure servers are suitably patched. Network activity is subject to security monitoring processes.

3.4 Change management forms part of the organisation's Project Management processes. A documented disaster recovery plan is in place and has been communicated to relevant staff.

3.5 However we also found some opportunities for improvement to existing arrangements. An IT Strategy is in place and is aligned with the corporate strategy. The Strategy is composed of individual tasks set out within a 5 year road map, however it does not document the resource requirements to complete each task. A software asset register is not maintained.

3.6 We reviewed the acceptance of the Information Security Policy by staff and identified that 30 of 138 staff members had

yet to confirm their acceptance of the policy. From a review of admin accounts, we identified one admin log-in which was shared by two members of the IT Team.

3.7 Although a disaster recovery plan is in place there is no regular testing of the effectiveness of the plan. Furthermore, back-up tapes are stored offsite, in a fireproof safe, however there is only one copy of the key to the safe.

3.8 An action plan is provided at section four outlining our observations, risks and recommendations. We have made five 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.	0
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

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

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

3.11 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 & Trossachs National Park Authority – IT General Controls

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: An adequately resourced IT Strategy is in place.				
1	An IT Strategy is in place and is aligned with the overall corporate strategy. The Strategy is composed of individual tasks set out within a 5-year road map, however the resource requirements to complete each task (Cost/Labour hours) have not been documented. Without clear resource requirements there is a risk that tasks are not appropriately prioritised or allocated the required resources at the outset of the task.	Management should consider quantifying the resource requirements for each task within the organisations 5-year road map.	**Medium**	**Response:** Management has considered and do not think it would be proportionate or useful to put specific resource estimates against the 5-year plan. The plan itself was developed within the context of our organisation's overall resource limitations and therefore already takes into account the constraints that we face. **Officer Responsible for Implementation:** Director of Corporate Services **Timescale for Implementation:** Complete

Title of the Audit: Loch Lomond & Trossachs National Park – IT General Controls

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: A Software Asset Register is in place.				
2	A Software asset register is not currently maintained. Although there are controls in place to prevent unauthorised software installations by staff, there is no register of the software deployed across the organisation. Without a software asset register there is an increased risk that unlicensed software installed on the estate is not identified.	Management should ensure that a software asset register is put in place. This should include (but not limited to) a record of the: - software title - version number - type of licence - number of licenses held - number of licences in use Thereafter steps should be undertaken to ensure that it is regularly reviewed for accuracy.	**Medium**	**Response:** The recommendation is acknowledged and will be actioned. The need for a Software Asset register was already included in our current 5 Year Strategy. **Officer Responsible for Implementation:** Information Systems Manager **Timescale for Implementation:** Before 31st March 2022

Title of the Audit: Loch Lomond & Trossachs National Park – IT General Controls

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Staff have been made aware of their Information Security responsibilities and these are understood and accepted.				
3	We reviewed the acceptance of the Information Security Policy by staff and identified that 30 of 138 staff members had yet to confirm their acceptance of the policy. There is a risk that staff are unaware of their Information Security responsibilities.	Management should review the Information Security acceptance records and ensure that all staff confirm their acceptance of the policy.	**Medium**	**Response:** The recommendation is acknowledged and will be actioned. Current processes in place to record acceptance will be reviewed. The policy is due to reviewed and updated in June 2021 and reissued to all staff. **Officer Responsible for Implementation:** Information Systems Manager **Timescale for Implementation:** Before 31st July 2021

Title of the Audit: Loch Lomond & Trossachs National Park – IT General Controls

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Each account is attributed to a named user.				
4	We identified one admin account which was not attributed to a named individual. This means these accounts could be used to access the network without being able to trace these actions back to a specific user. The use of unattributed user accounts therefore reduces accountability and increases the risk of the accounts being misused.	Management should ensure that, where possible, each account is attributed to a named user. Where generic accounts cannot be removed access to these accounts should be suitably controlled and use should be logged and monitored.	**Low**	**Response:** The recommendation is acknowledged and will be actioned A log has been set up to record the use of the generic accounts and will capture the name of person using the account, the Server/computer used on, the tasks the account was used for, time and date. **Officer Responsible for Implementation:** Information Systems Manager **Timescale for Implementation:** Complete – 19/04/2021

Title of the Audit: Loch Lomond & Trossachs National Park – IT General Controls

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Disaster recovery arrangements are regularly tested.				
5	A disaster recovery plan is in place however there is no regular testing of the effectiveness of the plan. Back-up tapes are stored offsite in a fireproof safe however there is only one copy of the key to the safe and is therefore a single point of failure. Without regular testing of the organisations disaster recovery plan there is an increased risk that business critical functions cannot be restored effectively, following a loss or interruption of IT.	Management should ensure that the disaster recovery arrangements are reviewed to ensure they are not reliant on a single safe key. Thereafter testing of the disaster recovery plan should be undertaken on at least an annual basis.	**Medium**	**Response:** The recommendation is acknowledged and will be actioned **Officer Responsible for Implementation:** Information Systems Manager **Timescale for Implementation:** Before 31st March 2022