Loch Lomond and The Trossachs National Park Authority

Internal Audit Report 2025/26

Management Information / Information Security

February 2026

Review Sponsor: Jane Kemp,

Head of Governance and Performance

azets.co.uk

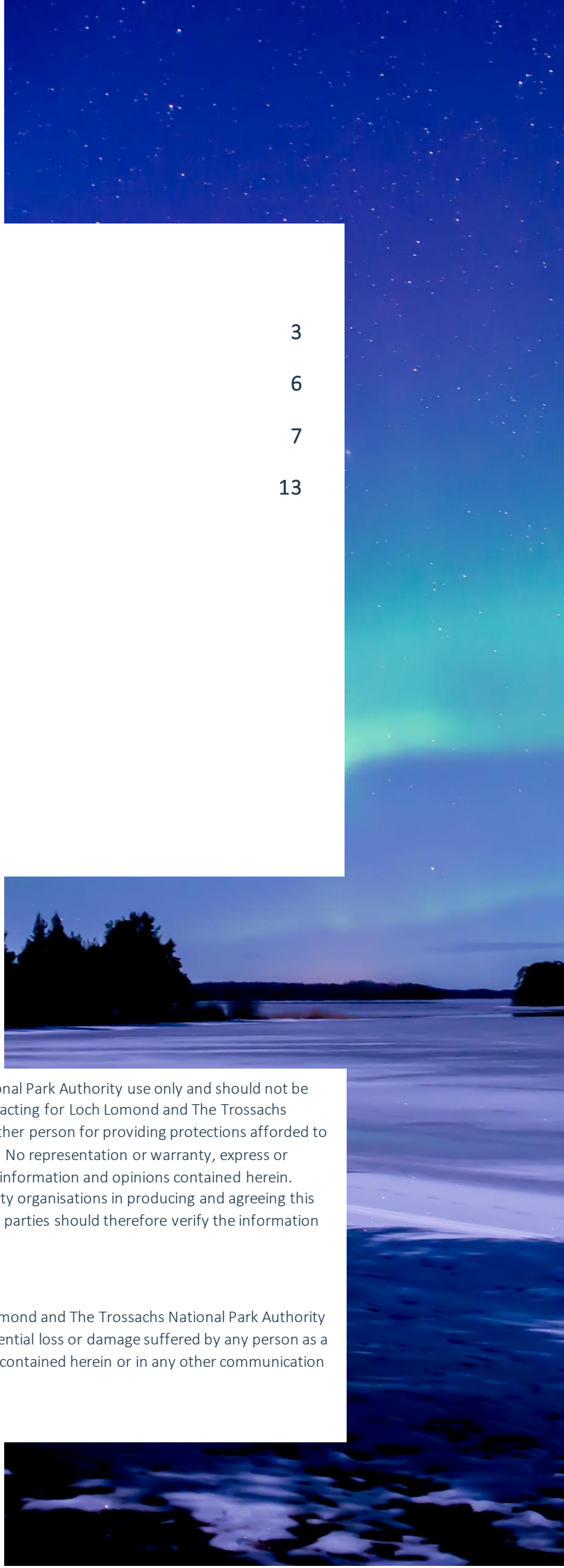


Table of Contents

Executive Summary

Conclusion

Audit Rating	Minor Improvement Required

The organisation does not use the term "Management Information" but does regularly use key information and data to inform decision making as and when required. This includes internal reporting, financial planning, and Board papers.

There are technical measures and controls for securely managing sources and repositories of key information. These controls include Role-Based Access Controls (RBACs), restricted external and guest access, monitoring of anomalous activity, Multi-Factor Authentication (MFA), and device encryption. Technical measures and controls are also supported with appropriate and up-to-date policies for Acceptable Use and Backup and Disaster Recovery (DR).

We noted a number of weaknesses, which, if addressed, would further strengthen controls for managing the information that the organisation holds. These include:

- A lack of overarching records of information used to inform decision making that is both complete and up to date. Existing processes rely on awareness of information required rather than a documented process.
- A lack of clear policy and procedure for information disposal. There were statements across documents relating to this stage within the information management lifecycle, however there is no dedicated policy and procedure for staff to refer to.
- Key policies, procedures, and supplementary documents for aspects of the information management lifecycle were overdue review. We noted that the organisation is already aware of this and that this had previously been flagged by the Audit and Risk Committee.

Background and scope

Effective management of information and its security is crucial for organisations in the modern, data driven environment. This involves not only safeguarding sensitive data against unauthorised access, loss or misuse but ensuring that information flows efficiently to support strategic decision making.

In accordance with the 2025-26 Internal Audit Plan, we have performed a review of Management Information/Information Security.

This review sought to determine whether there are adequate arrangements in place to manage and secure the information that the National Park Authority holds. This included the arrangements for managing the risks associated with the use of Artificial Intelligence (AI).

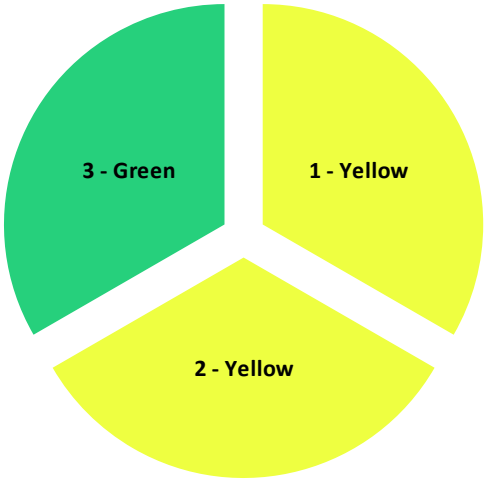
Key Contacts and Audit Team

Key Contacts	Audit team
Dougie Smith, Corporate Performance Manager *David Shepherd, Information Services Manager* *Helen Bowman, Legal Adviser*	*Martin Baird, IT Internal Audit Partner* *Ashley Bickerstaff, IT Internal Audit Manager* *Lara Boyaci, IT Internal Auditor* *Sam Keaveney, IT Internal Auditor*

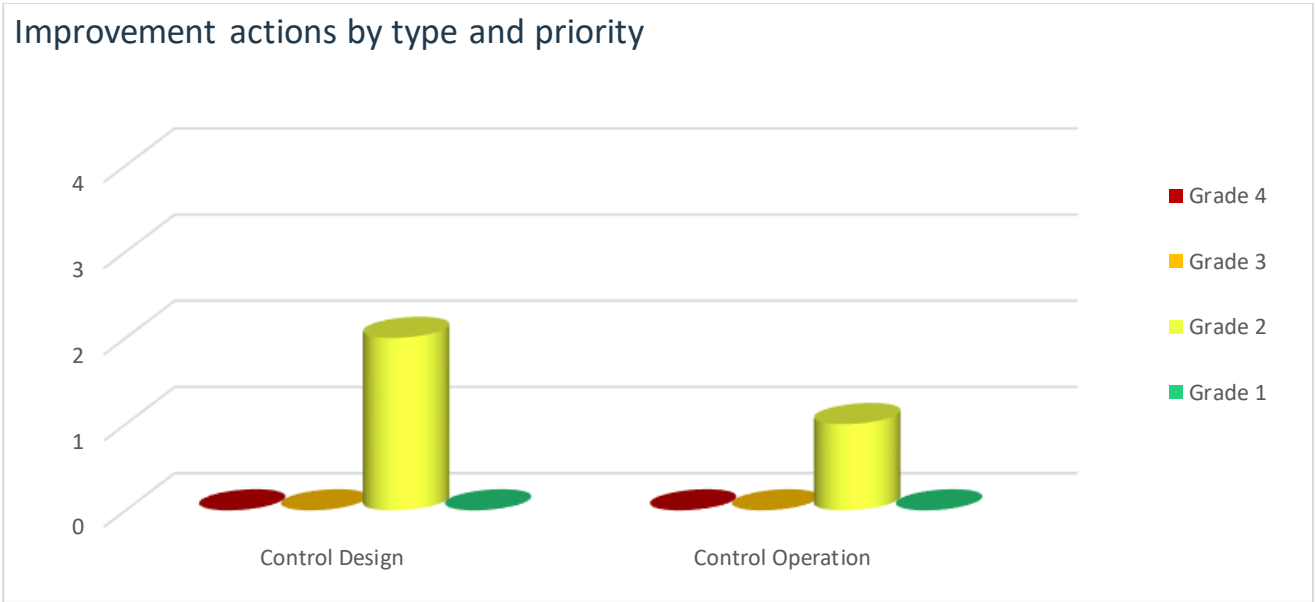
Acknowledgement

We would like to take this opportunity to thank all members of management and staff for the help, courtesy and co-operation extended to us during the year.

Control assessment



- 1. The organisation is aware of all management information produced and used for decision making purposes.
- 2. The organisation has governance in place for management information which includes policies and procedures for data collection, processing, storage and disposal as well as clear roles and responsibilities for information governance and data protection.
- 3. The organisation has implemented information security measures specifically technical controls for the sources/repositories of management information (e.g. infrastructure, application, network layers).



Three improvement actions have been identified from this review, one of which relates to compliance with existing procedures and two which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Good practice

- There are appropriate and up-to-date policies for Acceptable Use and Backup/Disaster Recovery (DR).
- There are various security measures and technical controls for sources and repositories of information, including, Role-Based Access Controls (RBACs), restricted external and guest access, monitoring of anomalous activity, Multi-Factor Authentication (MFA), and device encryption.

Areas for improvement

- There is no overarching record of information used to inform decision making that is complete and up to date. Existing processes rely on awareness of information required rather than a formal and maintained record.
- There is a lack of dedicated policy and procedure for information disposal.
- Various key documents have not been reviewed for several years, such as the Information Security Policy and Records Management Policy (which are specifically pertinent to the scope of this audit).

These are further discussed in the Management Action Plan below.

Impact on risk register

This review is not linked to a specific risk from the Corporate Risk Register (as at March 2025).

Cultural Observations

The culture within the area under review appears to be collaborative and places value on improvement. There is commitment to strengthening processes for management of information and its security as reflected within the technical controls and engagement throughout audit fieldwork. There is ownership of processes for this as identified through key documentation and during fieldwork meetings, however, the organisation has found this challenging due to resource constraints and workload priorities.

Management Action Plan

Control Objective 1: The organisation is aware of all management information produced and used for decision making purposes.

Yellow

1.1 Record of Information

Observation

The organisation does not use the term "Management Information / MI" and is not data-heavy with automated sets of information. The organisation produces and distributes required information as needed, such as for Procurement reports, Finance packs, reports to Executive, notes from Executive meetings and Board papers for strategic oversight.

There is no overarching record of all key information produced and used to inform decisions, nor has there been any steps to identify this information and the location, availability, currency, interdependencies, or information owner. We were informed by the Corporate Performance Manager that this is because the organisation does not consider it necessary for their size and because the organisation does not use information that is digitally generated with data flows. We noted that this was not consistent with the records management principles outlined in the Records Management Policy, which includes regular review and controlled retention of information.

There is a Retention Schedule which details the records used within the business, with information of the records used, the relevant activity, retention period trigger, retention period, disposal requirements, and reason for use. There are 22 tabs for each of the business functions, ranging from Communications to Corporate Management and Finance to Visitor Management. We noted that only a small number of the 22 tabs appear to have been updated in 2023 or 2024

While there are processes to enable identification and awareness of records, this was not reflected through to the information level. There is some visibility of information used to inform decision making, but this currently relies on having an existing understanding of information required rather than formal process to ensure a complete record of this is maintained.

Root cause analysis

There is no overarching record of information used to inform decision making that is complete and up to date as the organisation did not consider it necessary due to their size and lack of digitally generated information use.

Risk

The organisation may not have visibility of all key information required, therefore there is a risk that it does not have the information needed to inform decision making and is also unaware of how some information is used, retained and secured. This may result in ineffective decision making, inability to apply appropriate security controls or retention periods, and non-compliance with regulations such as UK GDPR.

Recommendations

Ref	Recommendation	Grade	Management Response	Action Owner and Due Date
1.1A	We recommend undertaking an exercise to identify all key information used across the organisation to inform decision making, using the Retention Schedule as the basis. The output of this should be a document which lists the information, its classification, where it is stored, how it is maintained, the retention period, the security controls required, and the owner of the information. We recommend that this is maintained as a live document, with supporting policy and procedure implemented to clarify the organisational requirements and responsibilities of staff.	2 (Design)	Accepted. We will undertake, as part of the wider review of our approach to records management, an exercise to consolidate all key information into one location and maintain it as a live document with processes and responsibilities made clear.	Information Manager 31/03/2027

Control Objective 2: The organisation has governance in place for management information which includes policies and procedures for data collection, processing, storage, and disposal as well as clear roles and responsibilities for information governance and data protection.

Yellow

2.1 Maintaining and Implementing Key Documents

Observation

We reviewed various Policies, Procedures and Guidance documents to identify the practices and governance arrangements for the collection, processing, storage, security and disposal of information.

There was no specific policy or procedure for information disposal. There were statements across documents with information disposal practices, however there was no single document with this information in one place for staff to easily refer to.

We also noted the following documents had not been reviewed or updated for a number of years:

- Information Security Policy which was last reviewed 2020.
- File Management Guidance which was last revised May 2020.
- Retention Schedule, with only a few of the 22 tabs having been updated in 2023 or 2024.
- Records Management Policy which was last revised Oct 2016 and last approved Feb 2017.
- Records Management Plan Submission Document dated 2024 and appears to be a draft.
- Record of Processing Activity, which is dated July 2019.
- Naming Conventions and Version Control Guidance which was last revised and approved 2020.

This was also observed for the Data Protection Policy and supplementary Procedure, which were last revised in October 2018 and April 2019.

We were informed during fieldwork that the organisation is aware various documents are overdue review and was previously highlighted by the Audit and Risk Committee. The responsibility for review and update sits with the Information Manager who was on sick leave during our audit fieldwork. We were informed during the close-out meeting on 21.01.26 that the Information Manager had since returned.

Root cause analysis

There is no information disposal policy or procedure as this is a gap that had not been identified. We were informed that as staff have been able to follow the disposal process across documents, the lack of policy or procedure had not been raised as an issue.

Policies and procedures are overdue review due to lack of resource and changes in staff responsible for oversight of documents. We were informed that reviews and updates have had to prioritise key documents due to internal staff changes and absences.

Risk

There is a risk that information is inappropriately managed or not disposed of correctly due to lack of specific disposal policy and procedure, and due to overdue review of key documents for managing the

information lifecycle. This may lead to unavailability of key information, insecure information or inadequate information used to inform planning and business decisions.

Recommendations

Ref	Recommendation	Grade	Management Response	Action Owner and Due Date
2.1A	We recommend implementing a policy setting out the expected approach to information disposal within the organisation, with a supporting procedure explaining the steps for staff to take for this to operate in practice.	2 (Design)	Accepted. Information disposal policy and procedure to be developed as part of the wider organisational approach to Records Management.	Information Manager 31/03/2027
2.1B	We also recommend reviewing the overdue policies, procedures, and guidance with priority to ensure that key documents remain appropriate and up to date.	2 (Operation)	Agreed. Relevant policy review to be undertaken and ensure they are in line with the revised organisational approach to Records Management.	Information Manager 31/03/2027

Control Objective 3: The organisation has implemented information security measures and specific technical controls for the sources/repositories of management information (e.g. infrastructure, application, network layers).

No weaknesses identified

We reviewed various policies and procedures containing the expected approaches to control access and protect information. This includes the:

- Information Security Policy with key roles and responsibilities, and high level practices for asset management, physical and environmental security, user access management, equipment security, network security management, mobile computing and teleworking, publicly available information, information handling, and information sharing.
- Information Security (IS) Acceptable Use Policy which sets out the expectations for use of the organisation's internet, email, telephone, information systems, and services. This contained practices for keeping accounts, passwords secure, systems and devices secure as well as outlining the appropriate use of email, internet, and telephone services.
- Backup and Disaster Recovery (DR) Policy which set out the approach to backup and DR of the organisation's data, servers, and information systems.

We assessed security measures and technical controls for the sources and repositories of information and noted that the following was in place:

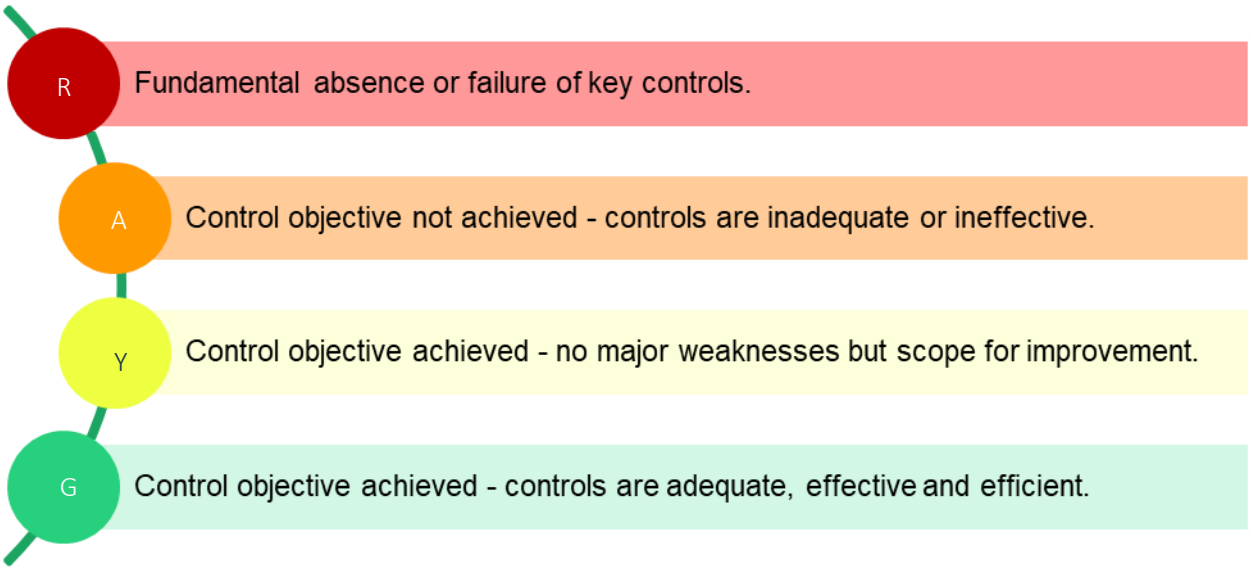
- Role-Based Access Controls (RBACs) for data stored within SharePoint. This is controlled via Security Policies, with membership roles prescribing access across different SharePoint sites.
- Restricted access for external or guest users. We noted this was set to the most restricted level of access, with only users assigned to specific administrator roles being able to invite guest users.
- Monitoring and reporting of anomalous activity via Microsoft Defender which integrates with M365 and Acumen Cyber Portal provided by cyber security partner (Acumen Cyber). There is also monitoring and dashboards for scanning cloud-based applications usage, threat analytics, incidents, and vulnerability management.
- Multi-Factor Authentication (MFA) for staff and administrators.
- Device encryption.

Appendix A – Definitions

Audit Ratings

Immediate major improvement required	•Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and objectives should be met.
Substantial improvement required	•Numerous specific control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives should be met.
Minor improvement required	•A few specific control weaknesses were noted; generally however, controls evaluated are adequate, appropriate and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Effective	•Controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.

Control assessments



Management action grades

4	•Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.
3	•High risk exposure - absence / failure of key controls that create significant risks within the organisation.
2	•Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.
1	•Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.