Cairngorms National Park Authority

Internal Audit Report 2022/23

Data Management

December 2022

Cairngorms National Park Authority

Internal Audit Report 2022/23

Data Management

Audit Sponsor	Key Contacts	Audit team
David Cameron, Director of Corporate Services	Lisa MacIsaac, Governance, Data & Reporting Manager	Neil Belton, IT Audit Director Ashley Bickerstaff, IT Audit Manager Heather Boyle, IT Auditor

Executive Summary

Conclusion

The Cairngorms National Park Authority (CNPA) does not have a complete suite of policies that addresses all expected policy areas for the lifecycle of data. Where policies are in place these have not been maintained.

CNPA has a high level migration plan documented for the migration of data into SharePoint, however, this does not fully detail all actions that are to be undertaken for the implementation or migration with ownership and completion dates set.

There is a significant link between the identification of requirements and risks for data management, the creation of adequate policies, and the embedding of suitable procedures. It is this connection of elements which CNPA have not established, and which could lead to additional work to reconfigure the SharePoint if not remediated.

Background and scope

Cairngorms National Park Authority (CNPA) is evolving the working practices and technology that underpins its systems and controls around data management. This evolution follows on from the organisation's response to COVID-19 and the changes as to how data is used and managed.

CNPA is migrating data and records from its' current network file share environment to SharePoint. The intention is that this will consolidate data into a cloud based, secure central location which, in turn, will provide a clearer view of the data that the organisation holds. SharePoint will be accessible to all staff whether working from an office or a remote location; supports collaborative working; and enables secure sharing of identified records with collaborating partners.

We have reviewed the adequacy of the organisation's approach to addressing data management challenges as part of the planned migration of data to SharePoint.

Control assessment

■ 1. Data lifecycle policies, standards and procedures have been reviewed and updated to support the strategic and operational use of SharePoint.
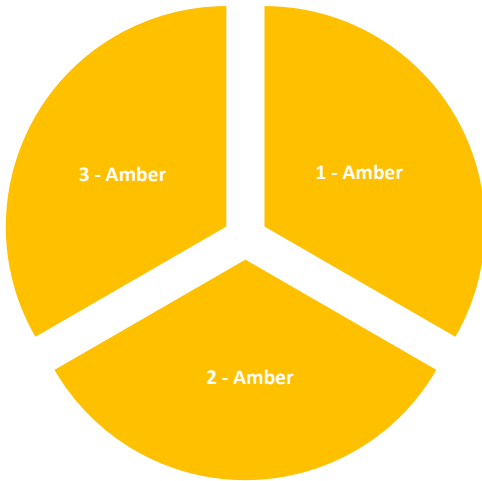
■ 2. The organisation has developed a migration plan for the move to SharePoint that addresses consolidation and security of data as well as training needs of staff.

■ 3. The planned implementation of SharePoint addresses key areas of information security such as; access controls, data labelling, security and retention.

Improvement actions by type and priority
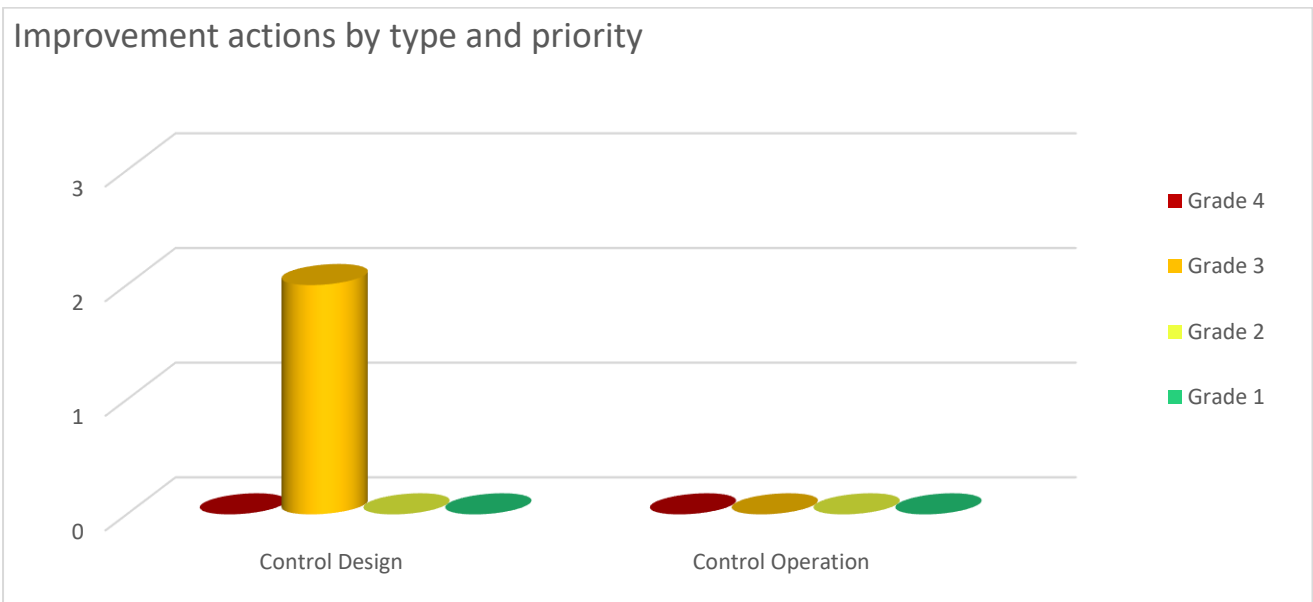
Two improvement actions have been identified from this review, both of which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Areas for improvement

We have identified areas for improvement which, if addressed, would strengthen CNPA's control framework. These include:

- CNPA does not address all expected policy areas within their policy suite. Where policies are in place they have not been maintained, with some not reviewed since 2016.

- CNPA have not fully identified and documented their solution requirements and the risks of data being migrated to and residing in the cloud.

- The organisation has not implemented sufficiently detailed planning for the migration to SharePoint.

These are further discussed in the Management Action Plan below.

Impact on risk register

The CNPA corporate risk register (January 2022) included the following risks relevant to this review:

- Risk A17 - Technical: Increasing ICT dependency for effective and efficient operations is not adequately backed up by ICT systems support.

- Risk A13 - Resourcing: CNPA IT services are not sufficiently robust / secure / or well enough specified to support effective and efficient service delivery.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Management Action Plan

Control Objective 1: Data lifecycle policies, standards and procedures have been reviewed and updated to support the strategic and operational use of SharePoint.

Amber

Control Objective 3: The planned implementation of SharePoint addresses key areas of information security such as; access controls, data labelling, security and retention.
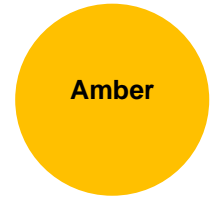
1.1 Policies and Requirements for Implementation

Key policies and procedures surrounding the lifecycle of data are not in place within CNPA.

An overarching ICT Policy includes references to acceptable use of internet and email, as well as electronic filing and disk space management; this policy has not been updated since January 2016. Policies addressing areas of data security, such as Access Control, Cloud and Data Security, and Data Labelling and Classification, are not addressed in existing policies.

There has been no work to update any policies with relation to the use of SharePoint. Policies that are in place are outdated; the organisation's Data Protection Policy and Data Security Breach Management Policy were last updated in September 2018, and the Email Policy in January 2016.

It is unclear how CNPA have defined technical requirements for migration to the cloud, as there is no formal documentation supporting this process and we would have expected that such requirements would be driven by relevant policy. Without these policies in place, there is a lack of clarity around how CNPA will embed their requirements into the configuration of SharePoint.

Risk

If policies and procedures for the storage and processing of data are not in place and maintained, there is a risk that CNPA will not be in a position to assess and identify their requirements for migration to SharePoint. This could result in the security of data not being in line with legal or organisational requirements, which may have financial or reputational consequences.

Recommendation

We recommend that CNPA review the current policy suite that is in place and develop and implement policies that address the following policy areas:

- Data Management
- Data Retention
- Information Transfer
- Cloud Security
- Data Protection

- Access Control
- Back-up and Resilience
- Data Labelling and Information Classification
- Acceptable Use
- Remote Access

We recommend that CNPA introduce a review cycle as standard for all policies, including those not directly related to the migration to SharePoint. The subsequent review and update process should be undertaken annually or in response to any significant changes or events.

The configuration of the SharePoint should be aligned to policy documentation, and take into account security and data protection needs, organisational structure requirements, and end-user experience expectations.

Once policies have been defined, this should allow the configuration of SharePoint in a manner which fulfils the organisation's requirements and facilitates expected usage and behaviour.

Management Action

Grade 3 (Design)

Recommendation agreed. This recommendation is in line with the established direction of our SharePoint Transition Project and we will incorporate the elements of the recommendation in a revised project plan. Management has suspended the full roll out of SharePoint to allow the technical requirements of transition and subsequent operation to be defined and agreed prior to full roll out and implementation of the system.

Note: we take the element of the recommendation on establishing a policy review cycle as a wider element of action, to be established more explicitly around all Park Authority policies.

Action owner:

Deputy Chief Executive, as senior sponsor of the SharePoint Transition Project and oversight of wider organisational development work required

Due date: 31 December 2023 for completion given breadth of elements of this recommendation

Control Objective 2: The organisation has developed a migration plan for the move to SharePoint that addresses consolidation and security of data as well as training needs of staff.

Amber
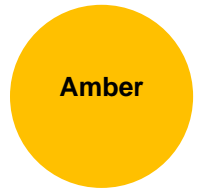
2.1   Migration Plan

CNPA have not established a detailed migration strategy or plan to steer the project. A timeline is in place, indicating the schedule of activities. This is high-level in nature and does not include owners or tracking to indicate if tasks have been completed as planned or if the migration is progressing on schedule. There is an understanding of the actions that will need to be completed as part of the project, from the benefits of migrating data gradually rather than in a single migration, to the need for training to be developed and sourced going forward. The migration plan, however, is not sufficiently detailed to document this.

There is engagement with a third party for the implementation of the SharePoint solution but it is not clear how engaged with the business CNPA's IT team have been in the development of the migration plan.

Risk

Without a robust cloud migration strategy, there is a risk that CNPA have not identified all actions required or the most appropriate methods of transition for the organisation, which may lead to data and file structures not meeting organisational needs and data protection obligations, or inappropriate management of data security and resilience.

Recommendation

In line with the update of policies and identification of requirements recommended in MAP 1.1, we recommend that CNPA establishes a cloud migration strategy or plan which takes into account how these requirements will be met by SharePoint and the actions required to configure the solution to do so.

Planning should be established at a lower level, with actions assigned responsible and accountable individuals as well as due dates. Continuous monitoring should be applied to ensure work is occurring in line with the schedule with reporting to a relevant governance group.

Management Action

Grade 3 (Design)

Recommendation agreed. Again, this is in line with the SharePoint transition project we have established, which had commenced preliminary work to identify requirements around this project.
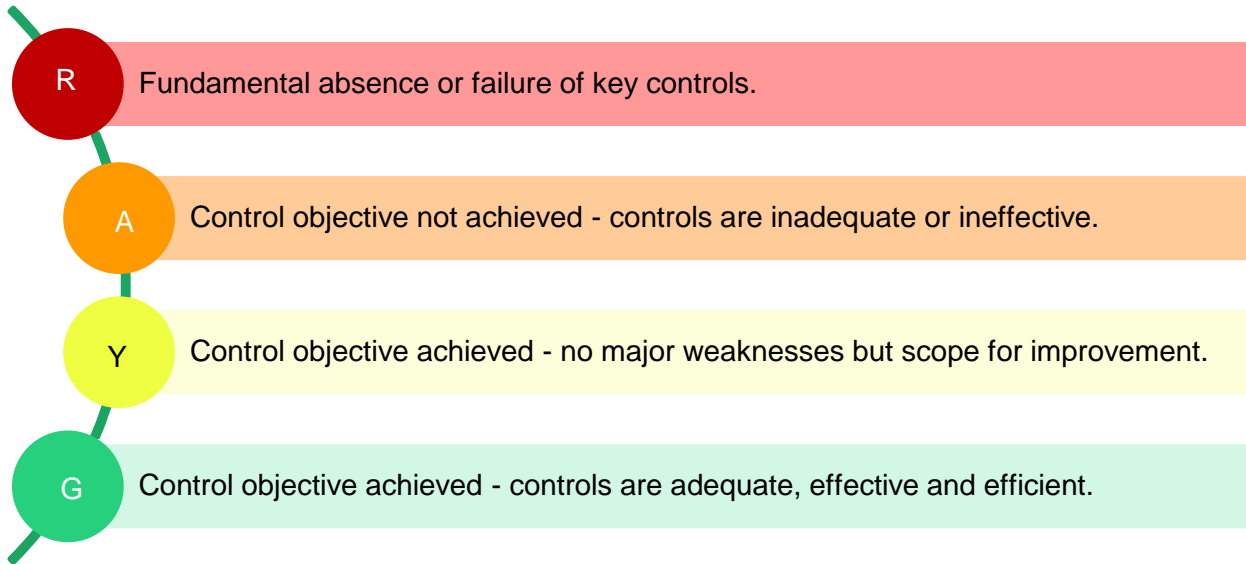
Action owner:

Deputy Chief Executive, as senior sponsor of the SharePoint Transition Project and oversight of wider organisational development work required
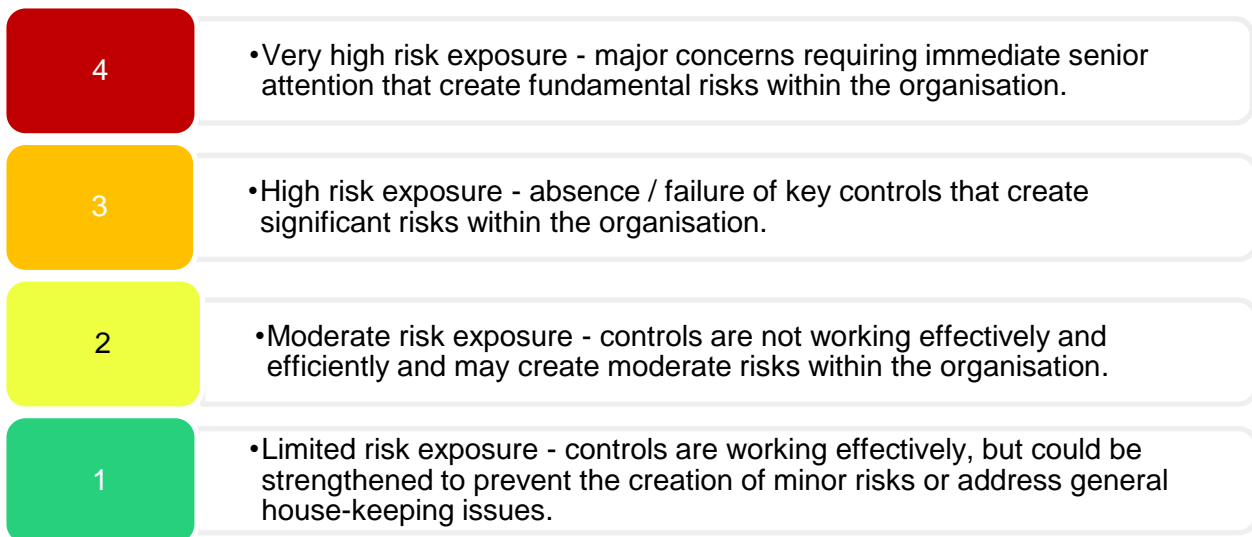
Due date: 30 April 2023

Appendix A – Definitions

Control assessments

R — Fundamental absence or failure of key controls.

A — Control objective not achieved - controls are inadequate or ineffective.

Y — Control objective achieved - no major weaknesses but scope for improvement.

G — Control objective achieved - controls are adequate, effective and efficient.

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.