Cairngorms National Park Authority

Internal Audit Report 2020/21

Data Management

February 2021

Cairngorms National Park Authority

Internal Audit Report 2020/21

Data Management

Audit Sponsor	*Key Contacts*	*Audit team*
David Cameron, Director of Corporate Services	*Vicky Walker, Office Services Manager* *Sandy Allan, IT Services Manager*	*Fraser Nicol, Partner* *Paul Kelly, Director* *Rachel Wilson, Assistant Manager*

Executive Summary

Conclusion

In 2018, the Authority took steps to improve their data management procedures. A policy update and file re-structure was planned to be carried out in May 2020 to improve further on the procedures implemented in 2018 however this has that have been delayed as a result of COVID-19.

We recommend that now the initial response to the pandemic has been addressed, the Authority should resume the activity initiated in January 2020. Specifically, we recommend that the Authority focuses on reviewing existing policies to ensure they are up to date, undertake activities to monitor compliance with policies, limit file structure modification rights to those who require it, and amend the file structure to reflect findings from the staff survey carried out in January 2020.

We have included an advisory section at the end of this report detailing our recommended approach for identifying the Authority's future IT needs and implementing cloud solutions.

Background and scope

It is important that organisations manage structured and unstructured data in an effective and efficient manner that support consistency of process. Structured data is typically identified as data that exists in tables and can be easily searched and analysed. Unstructured data is data that cannot be contained in a row/column model and which is difficult to search and analyse e.g. Word, Excel, PowerPoint, picture, video files etc.

It is particularly important to public bodies as there is a need to comply with several legislative requirements (GDPR, FoISA and EIR) that relies on the ability to be able to locate data and information in a timely manner.

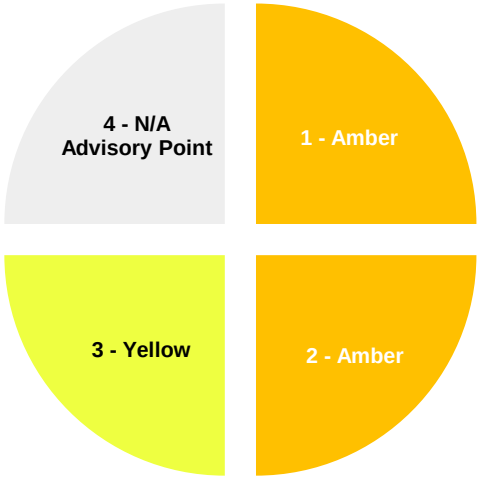
The organisation has been using its current network file share structure for approximately 5-6 years and, the working arrangements in response to COVID-19 has resulted in a renewed focus on having data and information easily and quickly accessible, ideally via cloud solutions such as SharePoint.

The Authority sought a review to provide assurance over the current approach to data management as well as an advisory/critical friend review of the planned processes for reviewing and changing file structures.

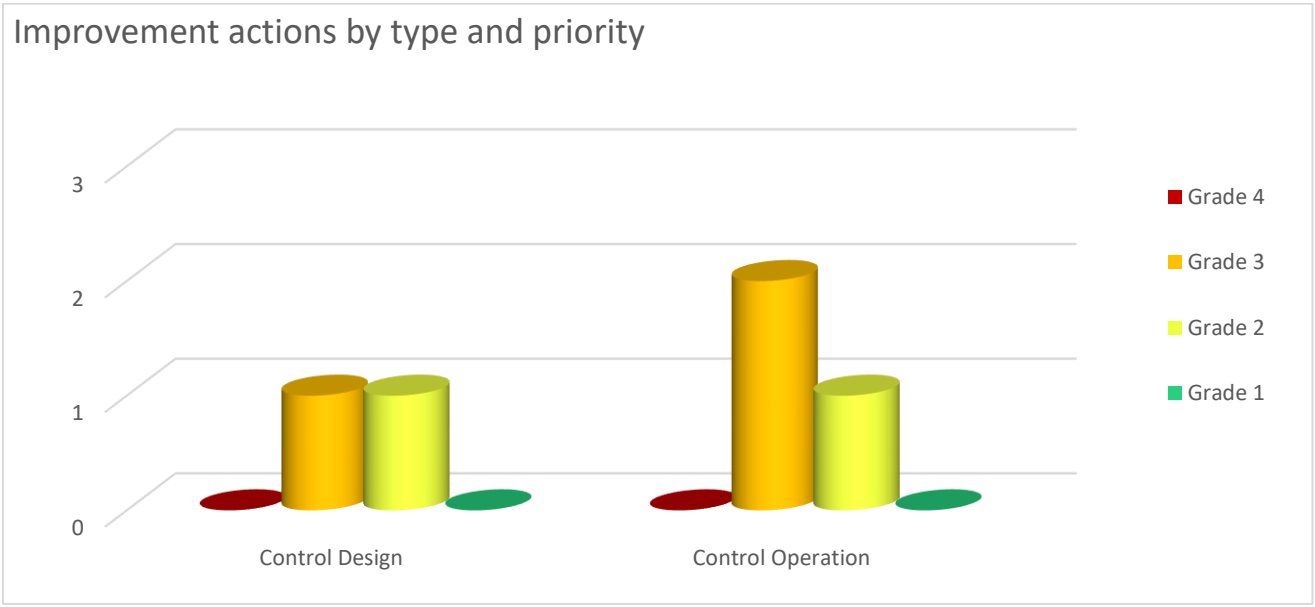
Our review considered the adequacy of current data management processes that support the organisation in responding to requests for information in relation to GDPR, FoISA and EIR.

The review also critically appraised the effectiveness of current data management structures at a key point in the change process.

Control assessment



- 1. There is agreed corporate policy / procedure for the storage of data and information on the corporate network.
- 2. Access controls to the network file shares are sufficient to prevent agreed file sharing structures being amended without authorisation.
- 3. The data structure are appropriate in supporting the agreed structures and these are adequate to allow the organisation to respond to requests for information in relation to data protection, freedom of information and environmental information requests.
- 4. Through discussion with management, we will critically appraise proposed approaches to changes in relation to data structures and migration to cloud services and how Brexit may impact on these.



Five improvement actions have been identified from this review, three of which relate to compliance with existing procedures, rather than the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Good practice

The Authority's procedures reflect good practice in the following area:

- The Office Services Manager conducted a staff survey in January 2020 to better understand how staff currently use the file structure and what they would like to be changed. Survey responses were collated, and the output was used by the Office Services Manager to create a proposed new structure for the shared file drive. This activity was put on hold because of COVID-19 however the responses gained from the survey will be helpful when the Authority resumes this activity.

Areas for improvement

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

- Update of existing policies to ensure they are current and consistent
- Implementation of compliance activities to measure staff compliance with policies
- Update of existing file modification permissions to limit this action to a small number of staff
- Creation of a subject access request response procedure

These are further discussed in the Management Action Plan below.

Acknowledgements

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

Management Action Plan

Control Objective 1: There is agreed corporate policy / procedure for the storage of data and information on the corporate network.

Amber

1.1 Update of data management policies

There are three policies which make up the corporate policy for data management: the Records Management Policy, the Information Security Policy, and the Data Protection Policy. The Records Management Policy documents roles and responsibilities of relevant staff, management of records, version control, data retention and disposal.

However, we found that although policies are required to be reviewed annually, the Records Management Policy had not been updated since February 2017 and the Information Security Policy was last updated in October 2016. Therefore, neither of these policies have been updated to ensure they reflect GDPR requirements.

There are also inconsistencies between the Records Management Policy and the Information Security Policy. For example, the Records Management Policy states that electronic records are available on an “open to all: need to know” basis meaning records are available for viewing to all staff unless specifically designated as sensitive. However, the Information Security Policy states that user access will be granted on a role-based, least privilege basis meaning that access is based upon the minimum level of information needed to fulfil your role.

Risk

There is a risk that, without up-to-date policies, there will be a lack of clarity for staff of what data management practices they should be following. This could lead to failure to comply with regulatory requirements and organisational controls.

Recommendation

We recommend that the organisation reviews and updates all three policies to ensure that they reflect the latest data protection legislation as well as current and planned organisational practices. Specifically, the Authority should ensure that information contained within each policy is consistent. The Authority should ensure that the owner for each policy is updated and going forward, it should ensure that policies are reviewed in line with the review frequency documented.

Management Action

Grade 2 (Design)

Recommendation accepted.

Action owner: Office Services Manager

Due date: 31 December 2021

1.2 Compliance with policy

The Records Management Policy states that the Authority will undertake an annual audit of both electronic and paper files to ensure compliance with records management best practice guidance, however we found that since the policy was implemented in 2017, this annual audit has not been conducted.

The policy also states that all electronic records folders and paper records folders will be appropriately marked with retention schedules and reviewed and disposed of accordingly. A data retention schedule is in place which details how long each type of file within each directorate should be held. Staff are required to include the retention within the folder name by adding "+YEAR". We sampled four directorate folders and found that whilst two of them had the retention included within folder names, two of them did not include retention times within file names.

Risk

Senior management is unaware that staff are not adhering to the policy which could lead to failure to delete data in line with the data retention policy and therefore failure to comply with data protection legislation.

Recommendation

We recommend that the Authority ensure that data audits are conducted annually in line with the policy. These audits should sample various directorates to ensure that storage and management of files adhere to the Records Management Policy. Specifically, this audit should consider compliance with data retention and disposal requirements, version control requirements and access and security requirements. The output of this audit should be documented and the Head of Service for each area should be given recommended actions as necessary.

We also recommend that the Authority evaluates the approach to ownership of folders and how compliance checks against the Records Management Policy are performed.

Management Action Grade 3 (Operation)

Recommendation agreed. While we note this is a high level, grade 3 recommendation, time is required to first implement other actions required by other recommendations prior to implementing data audits and compliance checks. Therefore an unusually long period to the due date for a grade 3 recommendation has been allowed for.

Action owner: Head of Organisational Development **Due date:** 30 June 2022

Control Objective 2: Access controls to the network file shares are sufficient to prevent agreed file sharing structures being amended without authorisation.

Amber

2.1 Access control

The Authority undertook a review of their shared network file structure in 2017 and this included a review of users who had amendment rights and as a result, only 3 or 4 users were given this level of access. Staff who wanted to create or amend folders were required to submit a request to the Admin Team via email.

However, we found that the number of individuals given this level of access has increased since 2017 and when the Authority moved to home working, it was decided that there should be one user per department with this level of access. As a result, there are now 26 users who have this level of access, out of a total staff of 67.

Risk

Users with inappropriate rights to make amendments may make modifications to the Authority's file structure that cause issues when searching for data to respond to subject access, freedom of information and environmental information requests. This could impact the organisation's ability to comply with regulatory requirements.

Recommendation

We recommend that the Authority reviews the list of users who can make modification to the file structure. The top level of folders i.e. folders for each directorate, should be locked down so that only a small number of users who require amendment rights can modify them. To support better management of file permissions for lower-level folders within each directorate, we recommend that each directorate is provided with access to create sub-folders within their respective top-level folder without having to ask IT or the Admin Team for permission.

We also recommend that requests for amendments to the top-level the file structure are submitted to the Office Service Manager who can make a decision on their justification.

Management Action

Grade 3 (Operation)

We agree with the overall thrust of the recommendation. We will review the structure and make a decision at which level of the folder hierarchy the folder structure will be locked down, and design / implement access procedures for teams to create lower level folders.

Action owner: Office Services Manager **Due date:** 30 June 2021

Control Objective 3: The data structures are appropriate in supporting the agreed structures and these are adequate to allow the organisation to respond to requests for information in relation to data protection, freedom of information and environmental information requests.

Yellow

3.1 Implementation of the proposed file structure

The Office Services Manager started work in January 2020 to review and restructure the R drive to meet users' needs. A survey was conducted to understand staff perspective on the ease of use of the current structure which revealed the staff would like to see the following be implemented:

- Use of consistent naming conventions
- Guide map of filing
- Easy access to templates

As a result, the Office Services Manager created a proposal for a new file structure. However, this activity was put on hold as a result of COVID-19. A risk was added to the corporate risk register to reflect the increased risk in data management as a result of the pandemic, however it is unclear when this activity will be resumed.

Risk

The current file structure does not reflect staff requirements which could result in frustration and an increased risk of workarounds being used which are not compliant with the corporate policy.

Recommendation

We recommend that the Authority resumes this activity to ensure that work to improve the management of data is not unnecessarily delayed following the Authority's initial response to the pandemic. The Authority should allocate resources to ensure that this activity can be carried out within a reasonable timescale.

Management Action

Grade 2 (Operation)

Recommendation agreed. We will design and implement a data integrity action plan and integrate that with our planning around staff phased return to the office to secure the integrity of our data.

Action owner: Office Services Manager with Business Continuity Steering Group

Due date: 31 August 2021

3.2 Creation of a subject access request procedure

There are currently procedure documents in place outlining the process to be followed when responding to freedom of information requests and environmental information requests. However, there is no procedure outlining the process to be followed when responding to a subject access request for GDPR compliance purposes.

The Authority received a complex subject access request in Summer 2020 and asked their data protection officer as a service (DPOaaS) provider to review their response to that request to allow them to identify any opportunities for improvement. At the time of our audit work in January 2021, the Authority had received the response and was reviewing this.

Risk

Staff are unaware of the process they should follow when responding to a subject access request which could lead to failure to meet the one-month response deadline. This could result in non-compliance with regulation.

Recommendation

We recommend that once the Authority have received the feedback from their DPOaaS provider, they create a subject access request procedure, or document the process within an existing procedure, if appropriate. The procedure should outline the following aspects:

- Roles and responsibilities when responding to requests
- Initial steps for acknowledging the request and verifying the identity of the individual
- Identifying what data is within scope
- How to search for data
- How data should be sent to the individual
- How requests will be logged and monitored by the Authority

Management Action

Grade 3 (Design)

Recommendation agreed and underway.

Action owner: Office Services Manager **Due date:** 30 June 2021

Advisory: Through discussion with management, we will critically appraise proposed approaches to changes in relation to data structures and migration to cloud services and how Brexit may impact on these.

Current Position

Remote Access

When the Authority first moved to a working from home environment as a result of the pandemic, their options for remote access were very limited. Limited licenses for the VMWare solution (12 licenses) were in place to allow staff to connect remotely to the corporate network. This meant that there were a number of staff who could not access the R drive. The Authority therefore decided to implement a temporary cloud storage solution called ZoHo. All staff can access ZoHo and store documents there whilst they are working from home. A select number of staff can still access the R drive through the VMWare and therefore act as a liaison point to provide copies of files for those staff who do not have access to the R drive. The Authority plans to migrate any data stored on ZoHo back on to the R drive once all staff regain access.

To increase the number of staff who can access the R drive remotely, the Authority has piloted use of a product called ZScaler, a remote network access solution which uses multi-factor authentication. There are currently about 15 members of staff using ZScaler. IT and the Director of Corporate Services are currently considering rolling this out to all staff however there are a number of devices which are not compatible with the product. There are therefore considerations to roll out new devices, as necessary, which are compatible with the ZScaler product to allow all staff remote access to the network.

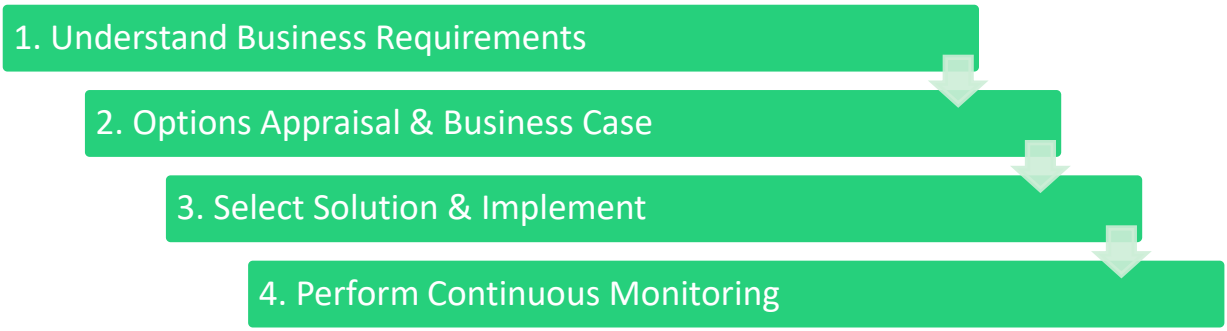
Cloud Solution

IT has written a paper on decisions to be considered to allow the Authority to migrate to cloud services where appropriate. The paper is currently in draft format and is high level, however it contains a section on decisions to be made within the next 6-12 months and possible options for the Wide Access Network (WAN) and Microsoft Office - the Authority currently uses Microsoft Office 2013. The paper is not yet finished but it is clear each option will include financial and organisation impact.

Recommendation

The past 10 months have highlighted that the organisation would benefit from improved operational resilience and technology solutions that support effective and efficient remote working. Taking into consideration the small number of IT staff within the organisation, it would be prudent to maximise technology “as a service” offerings in the medium and longer term. This includes moving specific services to managed service/cloud provision where it is cost effective to do so. This will reduce the technical skills needs and over-reliance on individual knowledge as this is transferred to third parties.

We recommend that the Authority takes the following steps when moving to a structure with a higher reliance on cloud solutions.



1. Understand the requirements of the business

   The Authority should look at what the needs of the business are in the following areas for their future IT environment:

   - Volume of data required to be held on a cloud solution
   - Collaboration needs of the business i.e. if they require the option to share data externally through the cloud solution
   - Identify the availability and recovery needs of the organisation
   - Identify the level of security and data protection needs of data that will be stored on the system. E.g. if personal data will be stored on the system, the organisation will need to consider regulatory requirements. The section on Brexit below, expands on this.
   - Identify the long-term goals for the Authority. i.e. is there the expectation that the Authority will move to Microsoft 365 and when would they want / expect this to happen?

2. Options Appraisal and Business Case

   - Once the Authority has identified the needs of the business, it should look for cloud solutions which meet these needs and compare them in a similar manner to the high-level draft paper produced by IT. The options appraisal should outline how each proposed solution meets the business needs in areas such as availability, storage space, security, as well as costs.
   - The options appraisal should be included within a business case which should be go through the relevant governance structure for authorisation, i.e. to the Director of Corporate Services, and if appropriate, the Finance and Audit Committee.

3. Select a solution and progress with implementation

   - When selecting a provider, the Authority should ensure that the necessary due diligence has been performed on the supplier(s). For example, the Authority should complete a Data Protection Impact Assessment, which considers where personal data will be stored, and a Security Assessment, which will assess whether the supplier's level of security meets the Authority's security requirements.

   - Once a solution has been selected, an implementation plan should be created which details how the Authority plans to move to the selected solution. The implementation plan should document timescales and owners for tasks, including:

     i. Clean up of the current file structure prior to migration to the cloud solution
     ii. Creation of a proposed structure for storage of files on the new solution
     iii. Creation of relevant policies and guidance documents for the new solution

4. Continuous Monitoring

    - Once the solution has been implemented, the Authority should continue to monitor use of the solution to ensure that staff comply with relevant internal guidance and operating procedures.

    - The Authority should establish formal contract management processes for all third party services provided.

Brexit

The transition period for Brexit ended on 31 December 2020. The EU has agreed to delay data transfer restrictions for at least four months although this might be extended to six months. The UK Government is currently seeking an adequacy decision. If the EU agrees to an adequacy decision, EU personal data will be allowed to be transferred and stored within the UK without the need for further action by individual organisations. However, if the EU does not agree to the adequacy decision, the Authority will need to ensure that the personal data of any EU individuals is either:

1. Stored within one of the countries that has been deemed adequate by EU GDPR; or
2. There is an appropriate solution in place with a country residing in a non-adequate country to ensure they comply with EU GDPR, e.g. standard contractual clauses.

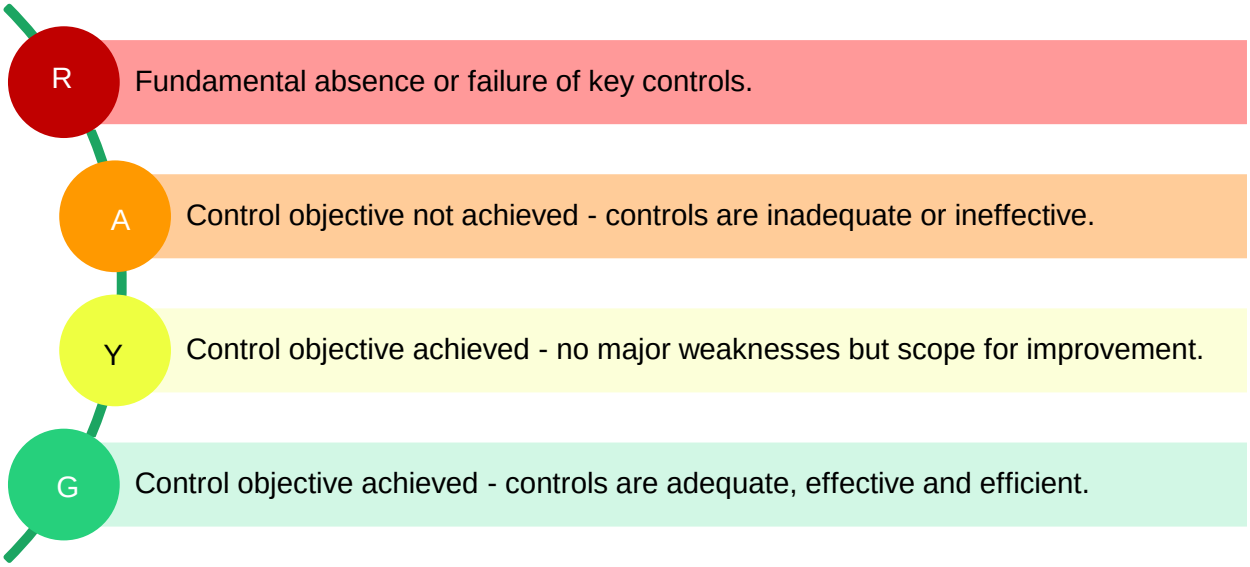
What this means for the Authority is that if they process the personal data of EU individuals, they will need to take steps to ensure that any cloud services provider complies with EU GDPR. Depending on an adequacy decision, this could mean taking additional steps if the cloud service provider stores data within the UK.

If the Authority only processes the personal data of UK citizens, which we currently understand to be the case, the Authority only needs to comply with UK Data Protection Act. This means that the Authority will need to ensure that data stored by cloud service providers resides within one of the countries deemed adequate by the UK, which currently includes countries within the EEA and those already covered by existing EU adequacy decisions. If the cloud provider does not store data within one of these countries, safeguards such as standard contractual clauses or binding corporate rules will need to be in place.

Most cloud service providers are aware of these requirements and have options in place to allow clients to select that they wish for their data to be stored within the EEA for these purposes, however this is something that the Authority will need to consider when selecting a service provider.

Appendix A – Definitions

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.