AZETS

Cairngorms National Park Authority

Internal Audit Report

Management Action Follow-up Part 1

2023/24

November 2023

Cairngorm National Park Authority

Internal Audit Report

Management Action Follow-up Part 1 – 2023/24

Introduction and background

Introduction

As part of the internal audit programme we have undertaken a follow up review to provide the Audit & Risk Committee with assurance that management actions agreed in previous internal audit reports have been implemented appropriately. This report summarises the progress made by management in implementing agreed management actions.

Scope

We have reviewed all open management actions and liaised with Cairngorm National Park Authority staff to obtain an update on their implementation progress. This included management identifying actions which were no longer applicable. For recommendations graded priority 3 or above, we request evidence to validate completion of any actions marked for closure by management.

For all actions raised by the prior Internal Auditor (BDO) we have aligned their risk assessments to the Azets risk grading structure (per Appendix 3).

## Action for Audit & Risk Committee

The Committee is asked to note the progress made by management in implementing agreed management actions. The Committee is also asked to consider and approve those actions for which revised timescales have been provided by management (these are detailed at Appendix 2).

Summary of progress

The table below shows the movement in the audit actions in the period from May 2023 to November 2023:

	Number of Actions
Open actions brought forward	35
Actions added to tracker	20
Total actions to follow-up	**55**
Actions closed	11
Actions no longer applicable	3
Open actions carried forward	**41**

Status of Actions as at November 2023

- Complete
- No Longer Applicable
- Partially Complete
- Incomplete
- Not Yet Due
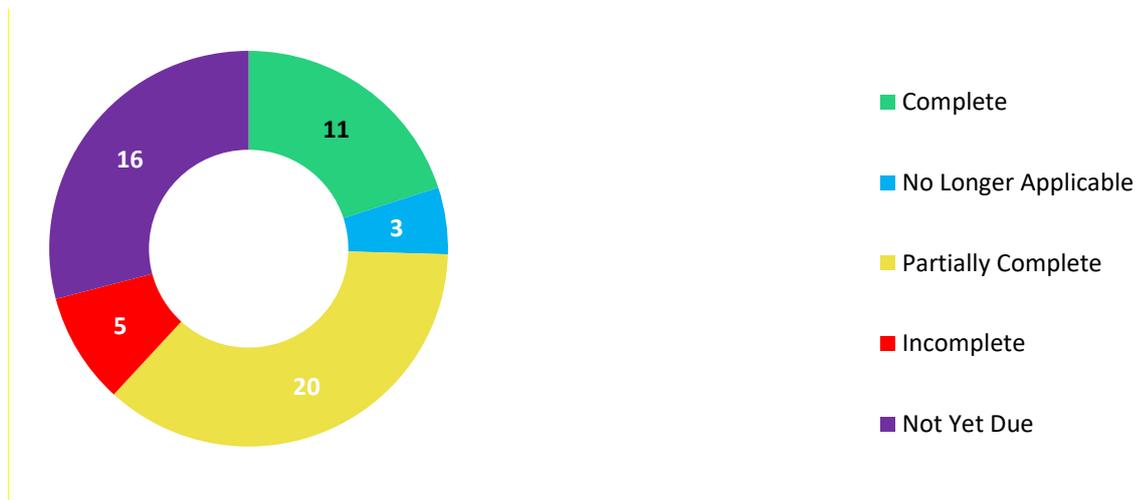
We have confirmed that 11 actions (20%) were competed in the period to November 2023, and three are no longer applicable (6%). 20 actions (36%) have been assessed as partially complete, five (9%) are incomplete and 16 actions (29%) were not yet due at the time of our validation work.

Further detail on all actions that have passed their current due dates for completion is included at Appendix 2.

We recommend that management retain a strong focus on clearing aged items in the coming months. We recommend prioritising the most aged items, dating back to 2016/17, and those that are grade 3 and grade 4.

Attention should then be paid to those remaining actions that have passed their original due date and those which will pass their due date for completion over the next period.

A summary of the status of actions by report is shown at Appendix 1.

Status by Grading
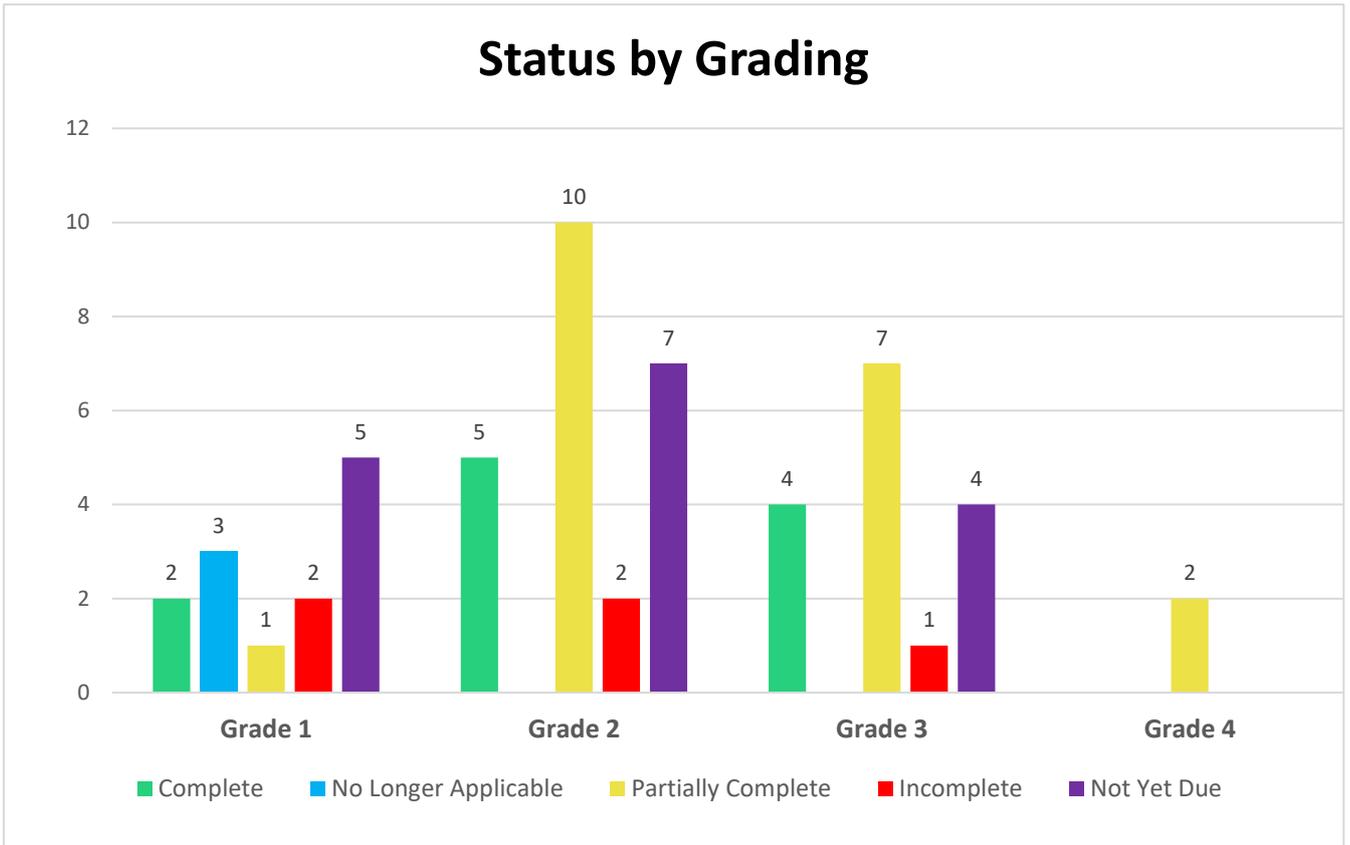
Open Internal audit actions

Of the 41 outstanding actions 25 (61%) have passed their original completion date.

15 of these actions have been assessed as a grade 1 or 2 (limited or moderate risk exposure), as a result, management should take a view on whether the organisation has the appropriate resource in place to move these actions forward, or are willing to accept the risk in place, in particular for those assessed as grade 1.

Appendix 1: Action status by report

Report title	Complete	NLA	Partially complete	Incomplete	Not Yet Due	Total
Financial Processes			1			1
Grant Funding & Management			1			1
2016/17 sub-total			**2**			**2**
Business Continuity Planning				1		1
2018/19 sub-total				**1**		**1**
Payroll Administration		2				2
Risk Management		1				1
Staff Objective Setting & Appraisal	1					1
FOISA and EIR Requests				1		1
2019/20 sub-total	**1**	**3**		**1**		**5**
Data Management			2	1		3
2020/21 sub-total			**2**	**1**		**3**
LEADER Programme			1			1
Financial Management and Reporting	1		1			2
Assurance Mapping of Major Projects			1			1
Cyber Security Review			2			2
ICT Strategy			4			4
Peatland Action Programme Set Up	4		3	1		8
2021/22 sub-total	**5**		**12**	**1**		**18**
LEADER Programme	1			1		2

Report title	Complete	NLA	Partially complete	Incomplete	Not Yet Due	Total
Performance Management			2			2
Data Management			2			2
Payroll and Expenses	4				5	9
2022/23 sub-total	**5**		**4**	**1**	**5**	**15**
Expenditure and Creditors					3	3
Risk Management					8	8
2023/24 sub- total					11	**11**
Grand totals	**11**	**3**	**20**	**5**	**16**	**55**

Appendix 2: Summary of outstanding actions past their original due date

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
2016/17 Financial Processes	We recommend that the Finance Management schedule is updated to provide detailed policies and guidance on all financial processes. These should be reviewed on an annual basis. We also recommend that clear roles and responsibilities demonstrating segregation of duties are documented within the guidance notes for all financial processes. We recognise that management have made progress in developing the schedule and that completion of this was delayed due to the implementation of the new Sage system.	Finance Manager	Low (Grade 1)	Jun-17	Mar 24	Desk instructions were updated prior to the commencement of the external audit in order to assist with walkthrough testing. However, these documents are relevant only to Finance staff.\n\nGuidance on procedures for the wider staff group are in need of update. Workshops were held in September 2023 to assist colleagues with financial governance.\n\nWe are working on streamlining our processes using work flows available through Microsoft 365. When these have been designed and established guidance documents will be prepared as part of the rollout of these new processes.	Partially Complete
2016/17 Grant Funding and Management	We recommend that the Grant Toolkit is completed, encompassing all processes in place for the awarding, recording and monitoring of grant funding. The toolkit should also clearly define the following:	Director of Corporate Services	Medium (Grade 2)	Sep-2017	Mar-24	Grant templates have been developed, including an award document and terms & conditions. Recent discussion around the organisation has identified a desire amongst colleagues for further guidance on making grant awards. Heads of Service are considering how to provide this support and the	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	- Actions to be taken when grant conditions are not being met or terms and conditions are breached. - The process for consideration of the risk and value of grant funding applications to determine the proportion of resource required to evaluate these; and - Review and scrutiny arrangements for progress reports provided by grantees.					potential for additional tailoring of templates to simplify the administration of small awards.	
2018/19 Business Continuity Planning	We recommend that CNPA develops a testing plan/schedule for BCP which should be reviewed regularly to ensure a strategic approach to testing is developed and implemented. This plan should ensure that varying categories of events are scheduled to be tested on a regular basis based upon likelihood and overall risk. A formal testing schedule should also be developed for the DRP. We note that the BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'tabletop' exercise. However, from discussions with management, it is understood that this is not	Director of Corporate Services	Medium (Grade 2)	Nov 2019	Aug 24	BCP is in need of update. It is the intention that consultancy will be engaged to develop and embed processes and procedures.	Incomplete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	achievable due to the size of the organisation. Therefore, Management should decide on the most suitable frequency of testing, and this should be detailed within the BCP. In addition, we recommend that the outcomes, lessons learned and required actions are formally documented, and thereafter reflected within the plan for each test.						
2019/20 FOISA and EIR Requests	We recommend CNPA review and update its Publication Scheme. We recommend CNPA reviews all information it holds with an aim to publish as much as possible to ensure transparency and reduce FOI requests.	Information Manager	Low (Grade 1)	Dec 20	Mar 24	Publication scheme will be updated in parallel the web development project	Incomplete
2020/21 Data Management	We recommend that the organisation reviews and updates all three policies to ensure that they reflect the latest data protection legislation and reflect current 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, recorded, and going forward, it	Information Manager	Medium (Grade 2)	May 2021	Mar 2024	This work is within the remit of Information Manager who is working through policies while making required improvements and developments.	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	should ensure that policies are reviewed annually in line with the review frequency documented.						
2020/21 Data Management	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 directorates each take ownership of their own folders and conduct more regular compliance checks within their own teams to ensure that their files comply with the Records Management Policy. The data owner for each file should be responsible for these checks.	Head of Organisational Development	Medium (Grade 3)	May-21	Mar 24	The appointment of our new Information Manager provides the opportunity to revisit this work. Our implementation of SharePoint is ongoing, and in due course we will set up automated retention rules to manage electronic documents. Consideration is being given to methods of document management that will reduce/ remove the need for hard copy paper records.	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
2020/21 Data Management	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	Office Services Manager	Medium (Grade 3)	Jun-21	Mar 24	The Information Manager will address the need for a policy and process around SAR and keeping abreast of the changes in UK legislation.	Incomplete
2021/22 Assurance Mapping of Major Projects	Management should put in place a project plan for implementation of the new project management approach. This may include the use of stage plans to help with maintaining flexibility over how the overall approach develops. In addition, management should ensure	Director of Corporate Services	Medium (Grade 2)	Sep-22	Mar 24	Project plan is in development	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	that this plan includes appropriate communications to explain any jargon or specific terminology.						
2021/22 Cyber Security Review	We recommend that CNPA should perform a risk assessment as well as a gap analysis of the current technology, policy and business environment, to identify the key cyber security risks. In conducting that risk assessment and gap analysis, CNPA should refer to recognised leading cyber security frameworks including the Scottish Government Cyber Resilience Framework. We recommend the introduction of a cyber risk register informed by the risk assessment and gap analysis, which includes input from all relevant stakeholders. We recommend that there is a process established for the ongoing identification and management of cyber security risks. We recommend that there is regular formal reporting of the organisation's cyber security posture to appropriate governance groups. This	Information Systems Manager	Medium (Grade 3)	Aug-22	Jun 24	While we are mindful of risks as part of the course of our day-to-day management of our IT resources, there has been a lack of formality in recording these risks. We are working to enhance our cyber-security rating and as part of this process we will document cyber-related risks.	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	should include information on incidents that have occurred (ideally on a summary or thematic basis to avoid the risk of weaknesses being widely publicised), actions being taken in response to incidents as well as assurance activity that has taken place, including the results of these.						
2021/22 Cyber Security Review	We recommend that CNPA establish procedures for handling cyber security events. These procedures may take the form of playbooks that specifically detail which actions should be taken in the event of a cyber-attack. We also recommend that following the development of the procedures CNPA should test the procedures to confirm that they enable an effective and efficient response to an event. We also recommend that management regularly reviews its technical cybersecurity posture. This should include ongoing assessment of the adequacy of technical solutions as well as their configuration to ensure that security risk from internal and external threats is minimised.	Information Systems Manager	Medium (Grade 2)	Dec-22	Jun 24	While we are mindful of risks as part of the course of our day-to-day management of our IT resources, there has been a lack of formality in recording these risks. We are working to enhance our cyber-security rating and as part of this process we will document these procedures.

Consideration is being given to a consultancy project towards development and implementation of the IT strategy and this work will include enhancement of our security procedures | Partially Complete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
2021/22 Financial Management and Reporting	Management should document and communicate the financial responsibilities of staff with financial authority, ensuring that all staff formally acknowledge their responsibilities.	Finance Manager and Financial Accountant	Medium (Grade 2)	Jun-22	Mar-24	Guidance on Delegated Levels of Authority was updated and published in May 2023. Copy of DLA document provided 06.09.23

Guidance on procedures for the wider staff group are in need of update. Workshops were held in September 2023 to assist colleagues with financial governance. Copy of presentation provided as evidence 26.10.23

We are working on streamlining our processes using work flows available through Microsoft 365. When these have been designed and established guidance documents will be prepared as part of the rollout of these new processes. | Partially Complete |
| 2021/22 ICT Strategy | We recommend that the next development of the IT and Data Strategy includes a financial strategy. This should set out, at a high-level, indicative capital and revenue costs associated with achieving expected outcomes from the strategy. This should be allocated for each financial year. This will allow management to make an informed assessment of the financial viability of the | Director of Corporate Services | Medium (Grade 2) | Sept 23 | Mar 24 | Development of the IT strategy will support preparation of the budget for 2024/25 | Partially Complete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	strategy and to ensure that financial requirements of the strategy are fed into annual budgeting/spending reviews.						
2021/22 ICT Strategy	We recommend that annual operational plans are developed which sets out a workplan for each financial year. This should include core operational tasks associated with maintaining a functioning IT environment as well as improvement and change activities relating to delivering the IT and Data Strategy. Planning in this manner will ensure that there are appropriate financial and human resources available to meet agreed IT and data priorities.	Information Systems Manager and Head of Finance	Medium (Grade 3)	Jun-22	Mar 24	The IT operational plan will, in future, follow naturally from the ICT strategy. While we are developing this strategic direction, operational aims have been set out to provide visibility of the IT team's aims and work scheduling.	Partially Complete
2021/22 ICT Strategy	We recommend that management explicitly document approvals of strategies within minutes of meetings. We recommend that management establishes formal governance arrangements for the approval of updates to the strategy as well as oversight of delivery. Governance over the IT &	Director of Corporate Services	Medium (Grade 2)	Mar-23	Mar 24	All strategy and policy documents are presented to both the Senior Management Team (at their fortnightly meetings) and the Board/ its committees. Approval is noted in the minutes of both meetings. The IT strategy will be subject to this governance process	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	Data Strategy should be the responsibility of an existing internal governance group						
2021/22 ICT Strategy	We recommend that the action plan within the IT and Data Strategy is updated to include action owners and delivery dates. There should be regular reporting to the SMT on the progress of the completion of actions. We recommend that when the new CNPA Corporate Plan is established a new IT and Data Strategy should be developed aligned with the corporate plan. The Strategy should also be reviewed with the approval of the Strategy by the appropriate oversight group fully documented and included within the document's version control.	Project plan = Information Systems Manager New IT Data Strategy = Director of Corporate Services	Medium (Grade 3)	Project Plan – Jun-22 Data Strategy – Sep-22	Mar 24	The Authority's strategic approach to ICT is under consideration. Initial discussions with our colleagues at Loch Lomond and the Trossachs National Park Authority (LL&T) have established a willingness from both organisations to extend the collaboration already happening; CNPA's strategic aims align with many of those expressed by LL&T. As we continue our conversation, action plans will be developed that include clear timeframes and project milestones to ensure effective delivery. Consideration is being given to a consultancy project towards development and implementation of the IT strategy.	Partially Complete
2021/22 Leader Programme	Management should ensure that feedback on CNPA internal processes is obtained and, where appropriate, fed into Scottish Government reviews on programme processes. In addition,	Director of Corporate Services	Medium (Grade 2)	Mar-22	Mar 24	Lessons learned have been applied in the preparation of the recent application to NLHF for Cairngorms 2030. An evaluation report was commissioned for the	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	management should develop a lessons learned action log and ensure this is monitored by a relevant person(s) within the CNPA management structure.					Development Phase of C2030 and this includes recommendations that will be carried forward into the Delivery Phase of the project.	
2021/22 Peatland Action Programme Set Up	Management should document the risks associated with the full-service approach and put mitigating controls in place to manage this within the risk appetite/tolerance of the CNPA Board. This should include obtaining legal advice in relation to the potential liabilities related to the full-service provision and award of contracts on behalf of the landowners. Roles and responsibilities of each of the parties subject to the full-service approach should be documented and communicated prior to services being provided. We recommend this is split by each step in the process, e.g. pre-application, application, project management and post project monitoring	Director of Nature and Climate Change	High (Grade 4)	Legal advice – Dec-22

Risk Map and action plan – Dec-22 | Jan 24 | This requirement is partially implemented. The Standard Legal Agreement has now been drafted by our lawyers and has been provided as evidence 19.10.23.

Risk mapping remains to be considered. | Partially Complete |
| 2021/22 Peatland Action Programme Set Up | CNPA should ensure the consistent treatment of Prior Notification costs, meaning that those should be reimbursed if incurred by | Peatland Action Programme Managers | Medium (Grade 2) | Nov-22 | Jan 24 | No update provided. | Incomplete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	CNPA and appropriately reflected in grant offer letters.						
2021/22 Peatland Action Programme Set Up	CNPA should ensure that the minimum controls, processes and documentation identified below are in place and being used. Detail in report.	Head of Service with Peatland Action Managers	High (Grade 4)	Feb-22	Jan 24	This requirement has been partially implemented. Some processes still need to be documented.

Peatland action programme documentation provided 27.10.23 | Partially Complete |
| 2021/22 Peatland Action Programme Set Up | Management should update the programme monitoring tools to provide sufficient information to manage the programme effectively including detailing progress with each of the stages within the core grant process for each project. Programme and action trackers used in other major projects/programmes could be used as a guide. In addition, arrangements should be put in place to ensure relevant programme and action trackers data is included in reports to the agreed governance structure recommended in MAP 5.1. Management should also review the actions within the Peatland Action Team action | Peatland Action Programme Managers | Medium (Grade 3) | Oct-22 | Jan 24 | No update provided. | Partially Complete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	tracker to ensure it is reflective of the current position and review the capacity of the Project Team and the availability of additional supporting resources to ensure that the prioritised actions are completed in an appropriate timeframe.						
2022/23 Data Management	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.	Deputy Chief Executive, as senior sponsor of the SharePoint Transition Project and oversight of wider organisational development work required	Medium (Grade 3)	Apr-23	Dec 23	A SharePoint transition plan has been developed and was agreed at the end of August 2023. The timeframe for migration is the end of December 2023.

An intranet for internal communication is in development and was launched in October 2023. | Partially Complete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
2022/23 Data Management	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.	Deputy Chief Executive	Medium (Grade 3)	Dec 23	Aug 24	The Information Manager is working on this as part of his review of policies.	Partially Complete

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
	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.						
2022/23 Performance Management	We support management's approach to developing a dashboard to support more frequent scrutiny and challenge by senior management. This should be implemented as soon as possible along with an agreed reporting structure, to ensure management receive sufficiently detailed updates in a timely manner.	Governance, Data and Reporting Manager	Medium (Grade 2)	Dec-22	Mar 24	The financial year 2022/23 has been a transition year between two corporate plans. During this period performance reporting has been largely qualitative in nature. We are now in the first year of the Park Partnership Plan, at the start of the Corporate Plan 2023-27, and potentially on the verge of commencing the delivery phase of Cairngorms 2030.

In order to assist in meeting reporting requirements in these three contexts, we are developing our approach to KPI management, and our budget process for 2024/25 will include the development of appropriate performance measures. We agree that visual summaries (a dashboard approach) provide a powerful view of performance and are seeking to develop these.

We have developed a job description for a new post | Partially Complete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
						(Knowledge Transfer Officer) to assist with this work.	
2022/23 Performance Management	Whilst developing the new corporate plan, management should ensure that this is supported by a sufficient mix of qualitative and quantitative measures and indicators that clearly define the proposed outcome of the activities being undertaken. In addition, management should look to increase the links to the National Park Partnership Plan, streamlining measurement and reporting processes.	Director of Corporate Services	Medium (Grade 2)	Mar-23	Mar 24	The financial year 2022/23 has been a transition year between two corporate plans. During this period performance reporting has been largely qualitative in nature. We are now in the first year of the Park Partnership Plan, at the start of the Corporate Plan 2023-27, and potentially on the verge of commencing the delivery phase of Cairngorms 2030.

In order to assist in meeting reporting requirements in these three contexts, we are developing our approach to KPI management, and our budget process for 2024/25 will include the development of appropriate performance measures. We agree that visual summaries (a dashboard approach) provide a powerful view of performance and are seeking to develop these.

We have developed a job description for a new post (Knowledge Transfer Officer) to assist with this work. | Partially Complete |

Report / Action	Recommendation	Action Owner	Grade	Original timescale	Revised timescale	Update November 2023	Status
2022/23 Leader Programme	To ensure grant processes are followed in a timely manner Management should consider whether contingency arrangements are required at key milestones and/or for key process steps within grant programmes, especially for those with limited staff resources.	Director of Corporate Services	Low (Grade 1)	Sept 23	Aug 24	BCP is in need of update. It is the intention that consultancy will be engaged to develop and embed processes and procedures.	Incomplete

Appendix 3: Audit risk categorisations

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.