Paper 5

Annex 1

Cairngorms National Park Authority

Internal Audit 2025/26

Follow Up Review

December 2025

Overall Conclusion

Weak

Table of Contents

Disclaimer

The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.

This report has been prepared solely for Cairngorms National Park Authority's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.

We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.

1. Executive Summary

Purpose of Review

The effectiveness of the internal control system may be compromised if Cairngorms National Park Authority (the Organisation) Management fails to implement agreed audit recommendations. Our follow up provides the Audit & Risk Committee with assurance that prior year recommendations were implemented within the expected timescales.

This review formed part of our 2025/26 Internal Audit Annual Plan.

Scope of Review

Our objective for this review was to assess whether:

- The Organisation has appropriately implemented any outstanding internal audit recommendations made in prior years.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation, and where appropriate sample testing.

1. Executive Summary

Conclusion

Overall Conclusion: Weak
Following our review, we can provide a weak level of assurance that the Organisation has endeavoured to implement internal audit recommendations raised in 2024/25 and the previous years. This is highlighted as three out of 12 recommendations were concluded to be fully implemented, five recommendations were found to be partially implemented, and the remaining four recommendations were not yet implemented.

Summary of Recommendations

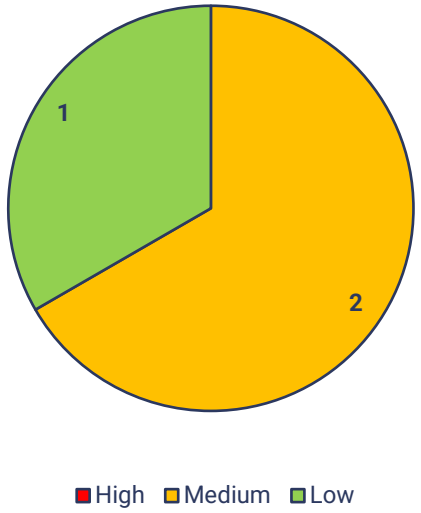
Grading of Recommendations	High	Medium	Low	Total
Appendix A - Not Implemented Recommendations	-	4	-	4
Appendix B - Partially Implemented Recommendations	1	4	-	5
Fully Implemented Recommendations	-	2	1	3

We have not included fully implemented recommendations as an appendix; however details of these recommendations are available upon request.

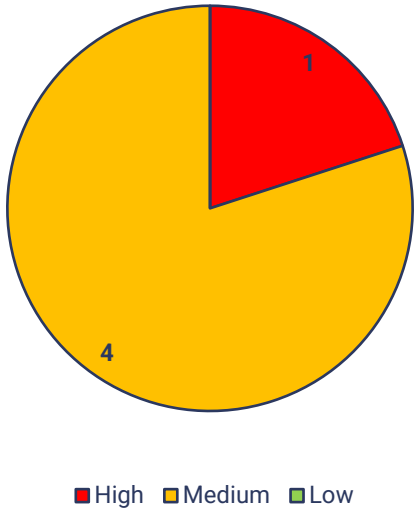
1. Executive Summary

Summary of Recommendations by Grade

Fully Implemented



Partially Implemented



Not Implemented

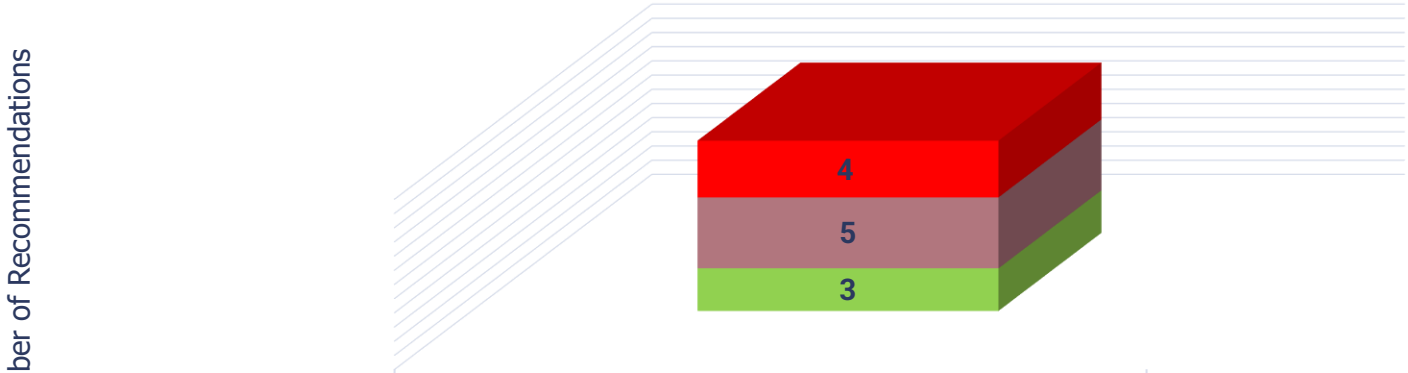
1. Executive Summary

Implementation of Recommendations – Summary of Implementation

Audit Area	Total	Not Implemented	Partially Implemented	Fully Implemented
Management Action Follow-Up Part 2 2024/25	**12**	4	5	3
Percentage of Total	**100%**	**33%**	**42%**	**25%**

1. Executive Summary

Breakdown of Recommendations by status of implementation, from 2025/26



	Management Action Follow-Up Part 2 2024/25
Not Implemented	4
Partially Implemented	5
Fully Implemented	3

2. Audit Arrangements

The table below details the dates of our fieldwork and the reporting of the audit area under review.

Audit Stage	Date
Fieldwork start	1 December 2025
Closing Meeting	11 December 2025
Draft report issued	18 December 2025
Receipt of management responses	5 January 2026
Final report issued	12 January 2026
Audit & Risk Committee	13 March 2026
No of audit day	5

2. Audit Arrangements

We detail below our staff who undertook the review together with the Organisation staff we spoke to during our review.

Wbg			
Partner	Graham Gillespie	Partner & Head of Internal Audit	gg@wbg.co.uk
Director	Peter Clark	Director of Internal Audit	pcc@wbg.co.uk
Senior Manager	Scott McCready	Senior Internal Audit Manager	smc@wbg.co.uk
Assistant Manager	CJ Scott	Internal Audit Assistant Manager	cjs@wbg.co.uk
Auditor	Dominic McCarthy	Internal Auditor	dmc@wbg.co.uk

Cairngorms National Park Authority			
Key Contacts:	David Cameron Louise Allen	Director of Corporate Services Head of Finance and Corporate Operations	davidcameron@cairngorms.co.uk louiseallen@cairngorms.co.uk

Wbg appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation.

Appendix A

Not Implemented Recommendations

A. Not Implemented Recommendations

Business Continuity Planning, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

In order to gain assurance that the BCP and DRP are effective in the event of a business disruption, it is important that the plans are tested on a regular basis.

The BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'table top' exercise. However, these have not yet been subject to formal testing, and there are currently no plans in place to test the BCP and DRP on a regular basis.

There is the risk that the BCP and DRP may not be effective, and that this will only become apparent when a disruption to a business critical process occurs.

Original Recommendation

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 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.

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
1.	The Organisation established and adapted business continuity plans during its response to COVID-19, however these have not been reviewed since after the pandemic. These plans are now outdated and require to be fully revised.	**Medium**	We reiterate the original recommendation.

A. Not Implemented Recommendations

Management Response	Responsibility and Implementation Date
The Authority's BCP is in need of update. It is the intention that consultancy will be engaged to develop and embed processes and procedures. Budget allocation will be provided for this in the 2026/27 budget.	*David Cameron / Louise Allen:* *September 2026*

A. Not Implemented Recommendations

Cyber Security 1, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

Our audit found that CNPA could enhance the cyber risk management practices and that the organization would benefit from greater formality in controls and processes to support more effective management of its cyber security risks.

Whilst we acknowledge that the organisation has taken positive steps to improve management of its cyber security risks, by recording high level cyber related risks on the Strategic Risk Register, there is no process for documenting and managing lower-level cyber risks.

Original Recommendation

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 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 he results of these.

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
2.	We note that formal risk assessments and gap analysis have not yet taken place. We do note that the Organisation has achieved Cybersecurity+ accreditation and further continues to develop and improve the IT arrangements.	**Medium**	We reiterate the original recommendation.

A. Not Implemented Recommendations

Management Response	Responsibility and Implementation Date
While we are mindful of risks as part of the course of our day-to-day management of IT resources, there has been a lack of formality in recording these risks. We are working to enhance the maturity of our cyber-security approach and as part of this process we will work to improve documentation and reporting. We have an informal register of operational risks used by the IT team, which will be developed and refined for wider review. Consideration will be given to the reporting channels appropriate to the ongoing risk position, the nature and safety of this reporting, together with the provision of information on responses to incidents.	*Responsible Officer: Louise Allen* *Implementation date: June 2026*

A. Not Implemented Recommendations

Cyber Security 2, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

Our high-level review in this area identified that CNPA has implemented technical solutions that assist in the mitigation and protection against cyber threats. Solutions have been implemented at a network and a device level. Firewalls are in place with the support of a third party for maintenance. Anti-virus is also in place which scans and updates regularly. A logging solution has been introduced to enhance the ability to understand what has happened in the event of an attack.

However, we found that while there are defensive measures in place, the current approach to cyber security is reactive in nature. A formal cyber security incident response plan is not in place to support the response to and management of service continuity in the event of an incident.

Original Recommendation

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.

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
3.	We note that formal procedures for handling cyber security events have not yet been developed. We do note that the Organisation has achieved Cybersecurity+ accreditation and further continues to develop and improve the IT arrangements.	**Medium**	We reiterate the original recommendation.

Management Response	Responsibility and Implementation Date
We have undertaken significant work to improve our security position over the past 18 months. We will continue to develop our approaches to include the establishment of procedures to handle cyber security events along with the regular testing and review of these procedures.	*Responsible Officer: Louise Allen* *Implementation date: September 2026*

A. Not Implemented Recommendations

Financial and Operational Planning 1, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

We confirmed through our discussions with management and review of the Operational and Financial Planning cycle documentation that the operational and financial processes are suitably aligned with regards to timescales, those involved and reporting through the governance structure.

CNPA creates annual operational plans by prioritising objectives included within the Corporate Plan 2023-27 and National Park Partnership Plan 2022-27, which were produced in consultation with Scottish Government. Once CNPA receives confirmation of its budget allocation from Scottish Government in December of each year the Heads of Service produce draft operational and financial plans for the year ahead, which are reviewed and approved by the Board in March in advance of the start of the financial year.

In addition, we reviewed the Budget Management and Monitoring document which was written by the Head of Finance and Corporate Operations and reviewed by Director of Corporate Services and Deputy Chief Executive in November 2023. This document sets out at a high level the above annual budget and operational process. However, the document does not clearly dictate the timelines for completion, roles and responsibilities of all parties involved, and expected documentation to be produced at each stage of the process.

Original Recommendation

CNPA should ensure that operational and financial planning process documentation clearly defines the roles and responsibilities of those involved, including timelines for completion and documentation requirements.

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
4.	Work to update financial planning process documentation has not yet been completed.	**Medium**	We reiterate the original recommendation.

A. Not Implemented Recommendations

Management Response	Responsibility and Implementation Date
The timelines for planning are set in response the requirements of Scottish Government. The Executive and Senior Management Team are fully aware of the relevant dates and required documentation. As we work through the development of the National Park Partnership Plan, and the ensuing Corporate Plan we will document the process undertaken, together with Roles and Responsibilities and timelines.	*Responsible Officer: Louise Allen* *Implementation date: September 2026 but dependent on progress towards completion of Corporate Plan 2027-2030*

Appendix B

Partially Implemented Recommendations

B. Partially Implemented Recommendations

Procurement, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

Prior to 2025 internal audit work was undertaken by a different provider who followed a different format which did not include details of the original finding. Instead, we have focused on the original recommendation, included below.

Original Recommendation

CNPA should undertake a full review of the procurement documentation held for each supplier. This should include confirming the last date of procurement exercise and determining contracts which require retendering. Management should seek to develop templates which set out the stages of the procurement journey, such as a template for briefing, supplier evaluation and ongoing contract management, in particular for routes 2 and 3 and as a minimum a checklist to be utilised for route 1. There should be clear documentation retained showing the current status of the procurement exercise, and once contractors have been appointed. As part of the work under MAP 1.1, CNPA should revise the current procurement policy to include a step-by-step process flow for the different thresholds, and a detailed explanation of the requirements of each step in the procurement route. This should also contain the required approvals and levels of authority required for each stage to ensure that staff are aware of their roles and responsibilities. This should include the process for noncompetitive actions including the documentation to be held and the thresholds in place. There should be a significant focus on training all staff with the updated policies, to ensure that there is consistent understanding and approaches across the teams. A central repository of all contract information should be maintained.

B. Partially Implemented Recommendations

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
1.	The Organisation has a Procurement Action Plan in place which it is currently using to track prior Procurement recommendations. In 2024, the Organisation hired a Procurement Officer, moving from previous use of an external provider for procurement services. This has worked to improve procurement processes across the Organisation. At the time of our review, the only outstanding point per the Procurement Action Tracker is the development of Procurement KPIs.	**High**	We recommend that the Organisation develop a set of formal set of procurement KPIs.
Management Response			**Responsibility and Implementation Date**
Procurement KPIs are currently under development.			*Responsible Officer: Louise Allen* *Implementation date: April 2026*

B. Partially Implemented Recommendations

ICT Strategy, Management Action Follow-Up Part 2 2024/25, March 2025			
Original Finding The IT and Data Strategy is not supported by a financial strategy. We did note that the CNPA budget for 2021/22 in March 2021 set out budget requirements to deliver a programme of transformation work which developed into the New Normal project. We also noted that the CNPA spending review in September 2021 set out the budget changes required to deliver the New Normal project with this including some elements of the IT and Data Strategy. These include Cyber Security software, website and records management augmentation and cloud-based ICT licensing. **Original Recommendation** 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 strategy and to ensure that financial requirements of the strategy are fed into annual budgeting/spending reviews.			
Ref	**Finding from our 2025/26 Follow Up**	**Grade**	**Recommendation**
2.	The IT Strategy was last reviewed in May 2025. The Strategy is detailed in many areas, however, some sections are still incomplete. The Executive Summary is currently blank, and the Roadmap included on page 40 is an empty template.	**Medium**	We recommend that the Organisation review and update the IT Strategy to ensure that all sections are completed.
Management Response			**Responsibility and Implementation Date**
The IT Strategy is currently under development			*Responsible Officer: Louise Allen* *Implementation date: September 2026*

B. Partially Implemented Recommendations

Data Management, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

Prior to 2025 internal audit work was undertaken by a different provider who followed a different format which did not include details of the original finding. Instead, we have focused on the original recommendation, included below.

Original 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.

B. Partially Implemented Recommendations

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
3.	Development of policies is underway, with policies covering Information Transfer, Data Protection, Acceptable Use and Remote Access in place, and with other key policies to be approved. The Organisation is working towards an updated Records Management Plan (RMP) under the Public Records (Scotland) Act 2011, to be submitted to The Keeper of Records by August 2026. Requirements for this plan include outstanding areas, such as management and retention of data, access control, and data back-up and resilience.	**Medium**	We recommend that the Organisation continues to update the key policies as well as update the Records Management Plan.

Management Response	Responsibility and Implementation Date
The finding noted above reflects the Park Authority's current position and aspirations.	*Responsible Officer: Paul Davison, Information Manager* *Implementation date: August 2026*

B. Partially Implemented Recommendations

Performance Management, Management Action Follow-Up Part 2 2024/25, March 2025			
Original Finding Prior to 2025 internal audit work was undertaken by a different provider who followed a different format which did not include details of the original finding. Instead, we have focused on the original recommendation, included below. **Original Recommendation** 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.			
Ref	**Finding from our 2025/26 Follow Up**	**Grade**	**Recommendation**
4.	The Organisation has extracted and formatted the information it wants to include in the dashboard in terms of delivery against its National Park Partnership Plan objectives. The Organisation is looking to find the correct mechanism for a 'live' dashboard which can become a part of more regular information management processes.	**Medium**	We reiterate the original recommendation. The Organisation should consider using PowerBI's functionality as a live dashboard.
Management Response			**Responsibility and Implementation Date**
The finding noted above reflects the Park Authority's current position and aspirations.			*Responsible Officer: David Cameron* *Implementation date: September 2026*

B. Partially Implemented Recommendations

Financial and Operational Planning 2, Management Action Follow-Up Part 2 2024/25, March 2025

Original Finding

We confirmed the Corporate Plan 2023-27 sets out the outline budget and forward financial projections for its objectives, including operational areas, specific projects and staffing resources. However, through discussions with management and review of the financial planning process, we noted that as CNPA receives an annual budget from Scottish Government management only create detailed financial plans on an annual basis and the forward financial projections included within the Corporate Plan have not been updated since its development to take account of any known changes.

Further, we confirmed that as part of the financial planning process, CNPA is required to produce financial plans for a range of budget scenarios for the Scottish Government. We reviewed the Budget Model 24/25 workpaper and confirmed that it sets out three budget movement scenarios, considering the impact of a 0%, 10% and 20% reduction in budget. However, the scenario plans are only developed for the forthcoming year and have not been created for the lifetime of the Corporate Plan 2023-27.

It is considered good practice to develop medium to long term financial plans that outline a range of clear assumptions and the implications of these on future activities.

Original Recommendation

CNPA should consider developing scenario plans for all future years of the Corporate Plan 2023-27 objectives and reviewing these as part of financial planning processes to ensure continued relevance. This could include utilising key assumptions and adjusting these to account for different scenarios, this may also assist in advancing planning processes and improving the spending cycle.

B. Partially Implemented Recommendations

Ref	Finding from our 2025/26 Follow Up	Grade	Recommendation
5.	The Organisation has focused on developing scenarios around the entirety of the budget position to understand any potential budget pressures. These long-term scenarios span corporate plan periods rather than being limited by the end of the current corporate plan timeframe. Scenario planning is still at an early stage, with various scenarios based on key assumptions to be developed. The Finance Team are working on additional information which will present the budget position against: 1. Commitments including pay and running costs; 2. Policy delivery priorities; 3. Other desirable project support / investments / actions	**Medium**	We recommend that the Organisation continue to develop it's budget scenario planning.
Management Response			**Responsibility and Implementation Date**
The finding noted above reflects the Park Authority's current position and aspirations.			*Responsible Officer: Louise Allen* *Implementation date: March 2027*

Appendix C

Grading Structure

C. Grading Structure

For each area of review, we assign a grading in accordance with the following classification:

Assurance	Classification
Strong	Controls satisfactory, no major weaknesses found, some minor recommendations identified
Substantial	Controls largely satisfactory although some weaknesses identified, recommendations for improvement made
Weak	Controls unsatisfactory and major systems weaknesses identified that require to be addressed immediately
No	No or very limited controls in place leaving the system open to significant error or abuse, recommendations made require to be implemented immediately

For each recommendation we make we assign a grading either as High, Medium, or Low priority depending upon the degree of risk assessed as outlined below:

Grading	Risk	Classification
High	High Risk	Major weakness that we consider needs to be brought to the attention of the Audit & Risk Committee and addressed by Senior Management of the Organisation as a matter of urgency
Medium	Medium Risk	Significant issue or weakness which should be addressed by the Organisation as soon as possible
Low	Low Risk	Minor issue or weakness reported where Management may wish to consider our recommendation

Appendix D

Assignment Plan

D. Assignment Plan

Purpose of review

The effectiveness of the internal control system may be compromised if management fails to implement agreed audit recommendations. Our follow up work will provide the Finance, Audit & Risk Committee with assurance that prior year recommendations are implemented within the expected timescales.

This review forms part of our 2025/26 Internal Audit Annual Plan.

Scope of review

Our objective for this review is to assess whether:

- The Organisation has appropriately implemented any outstanding internal audit recommendations made in prior years.

Audit Approach

Our approach to the review will be:

- Review outstanding recommendations and gain audit evidence to ensure that these have been addressed by the Organisation.

Potential Key Risk

The potential key risk associated with the area under review is:

- The Organisation does not address the areas of concern which may significantly affect its ability to continue to operate.