Paper 2

Annex 1

Cairngorms National Park Authority

Internal Audit
2025-26

IT Disaster Recovery

May 2026

Advisory Review

Table of contents

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. Every sound system 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

Overview

Purpose of review

The purpose of this advisory review was to assess Cairngorms National Park Authority's (the Organisation's) IT Disaster Recovery arrangements in the context of current hybrid working, cloud-based services, and recent digitisation. The review focused on the practical effectiveness of recovery planning, supporting documentation, and mitigation measures, providing pragmatic recommendations to strengthen IT resilience going forward.

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

Scope of review

Our objectives for this review were to review and advise on the Park Authority's IT Disaster Recovery arrangements, supporting the development of proportionate processes and documentation aligned to its systems, services, and operational requirements. Our objectives for this review were to assess if:

- The Organisation has a current and documented IT Disaster Recovery approach appropriate to its systems, services, and operational needs.
- Roles and responsibilities for IT recovery are clearly defined, communicated, and understood by relevant staff.
- Critical IT systems, including cloud-based SaaS, on premises systems, and specialist platforms such as Geographic information system (GIS), are identified and included in recovery planning.
- Backup arrangements are sufficient, reliable, and aligned with operational requirements, including clarity over third-party responsibilities.
- Recovery expectations, including Recovery Time Objectives and Recovery Point Objectives, are established and aligned to business

1 Executive summary

priorities.

- Resilience and mitigation measures are in place to reduce the likelihood and impact of IT service disruption.
- Testing on recovery arrangements can be carried out in a proportionate and pragmatic way, with lessons from tests and past incidents applied to strengthen plans.
- IT Disaster Recovery planning considers cyber-related incidents, including the ability to respond to ransomware, data corruption, or cloud service disruption, and that mitigation and recovery measures are appropriate.

We also considered the following areas as part of the review:

- The organisation's IT Team's understanding of their approach to disaster recovery, and associated operational arrangements in place, including arrangements shared with Loch Lomond and the Trossachs National Park Authority, and whether there are control gaps in these practices.
- Whether back-up arrangements in place within current operations are sufficient, reliable, and aligned with operational requirements, including clarity over third-party responsibilities.
- The IT team's recovery expectations in the event of any loss of systems.
- The IT team's understanding of resilience and mitigation measures in place or planned to mitigate the impacts of any service disruption
- The Organisation's current approach and controls regarding cyber security.
- The extent to which the Organisation has developed a written IT Disaster Recovery approach documenting these operational

1 Executive summary

arrangements.

Limitation of scope

There was no limitation of scope.

1 Executive summary

Background

Background and Context

The Organisation commissioned this advisory review to consider its IT Disaster Recovery arrangements in the context of increasing reliance on cloud-based services, hybrid working practices, and continued organisational growth. The review formed part of the 2025/26 Internal Audit Plan and was designed to support the development of proportionate and practical IT recovery capabilities aligned to the Organisation's operational needs.

This was a forward-looking, advisory engagement. Rather than providing formal assurance over control effectiveness, the review focused on understanding current arrangements, identifying gaps, and supporting the development of a structured and sustainable IT Disaster Recovery approach. Through this process, we engaged with a range of stakeholders across the Organisation, including IT, data management, planning, GIS, and operational programme teams, to build a holistic view of systems, dependencies, and recovery expectations.

As part of this advisory approach, we have raised a number of Action Points to support the development and prioritisation of IT Disaster Recovery arrangements, alongside a small number of Observations reflecting areas for further consideration as arrangements mature. Please refer to **Section 2: Action Points** and **Section 3: Observations** for further information.

To support ongoing development, we have also provided example templates and supporting materials to assist in documenting IT Disaster Recovery arrangements. These are intended to act as practical starting points and can be adapted by the Organisation to reflect its size, structure, and risk appetite.

IT Disaster Recovery Framework and Documentation

The review considered the extent to which the Organisation has established a defined and documented IT Disaster Recovery framework. This included discussions around existing documentation, historical arrangements, and the degree to which recovery knowledge is currently captured or held within individuals.

1 Executive summary

We explored how a structured IT Disaster Recovery approach could be developed in a proportionate way, including consideration of key components such as system inventories, recovery steps, roles and responsibilities, and supplier dependencies. The importance of maintaining a clear, accessible, and regularly reviewed document was discussed as a key enabler of effective recovery.

Systems, Backups and Recovery Priorities

We examined how the Organisation identifies and manages its critical IT systems, including cloud-based SaaS platforms, on-premise infrastructure, and specialist systems such as GIS and planning platforms. This included consideration of how system criticality is understood across services and how this aligns to operational priorities.

The review also considered current backup arrangements across both cloud and on-premise environments, including Microsoft 365 and locally hosted systems, alongside recent infrastructure changes to support resilience and failover. In parallel, we explored recovery expectations, including how quickly systems would need to be restored and the extent of acceptable data loss, and how these expectations align with business needs.

Dependencies on third-party providers and shared services were also considered, including the extent to which responsibilities for backup and recovery are defined, understood, and supported by appropriate assurance.

Resilience and Mitigation Measures

The review explored existing resilience and mitigation measures designed to reduce the likelihood and impact of IT disruption. This included consideration of cloud adoption, device management through Microsoft Intune, endpoint security through Microsoft Defender, and infrastructure changes such as virtualisation and failover capabilities.

We discussed how these measures contribute to overall organisational resilience, alongside the role of alternative working arrangements and dependency management in maintaining service continuity.

1 Executive summary

Testing and Exercising

We considered the Organisation's current approach to testing IT Disaster Recovery arrangements. Discussions highlighted the extent to which recovery activities have been validated in practice and explored pragmatic approaches to testing, including scenario-based exercises and targeted technical recovery tests.

The importance of proportionate and repeatable testing was discussed as a mechanism to build confidence, identify gaps, and support continuous improvement over time.

Cyber Incident Recovery

The review also considered how IT Disaster Recovery arrangements align with cyber-related incident scenarios, including ransomware, data corruption, and service disruption. This included discussion of existing cyber security controls and certifications, alongside the Organisation's ability to recover systems safely following a cyber incident.

We explored the distinction between incident response and disaster recovery, and how these should operate together to support both immediate response and longer-term recovery.

Prioritisation of Recommended Actions

The Action Points identified through this advisory review are interrelated and should be progressed in a structured sequence rather than as standalone improvements. Given the current maturity of arrangements, which are largely based on informal knowledge and operational understanding, the initial focus should be on establishing a clear baseline structure before progressing into validation, refinement, and specialist areas.

The prioritisation below reflects dependency, practicality of implementation, and the need to establish foundational clarity before progressing into more advanced resilience and testing activities.

1 Executive summary

Recommended Prioritisation Order

1. **IT Disaster Recovery Framework and Documentation**
   Establish a consolidated and practical IT Disaster Recovery framework to capture current knowledge, define core processes, and provide a consistent reference point for all recovery activity.
2. **System Criticality, Prioritisation and Recovery Expectations**
   Define and agree critical systems and services, including SaaS, on-premise and specialist platforms, and align these to agreed recovery priorities and indicative recovery expectations.
3. **Backup Arrangements and Third-Party Assurance**
   Confirm and document backup coverage across all environments, with clear articulation of internal versus supplier responsibilities and appropriate assurance over recovery capability.
4. **Testing and Exercising of IT Disaster Recovery Arrangements**
   Introduce proportionate and structured testing, starting with scenario-based exercises, to validate recovery assumptions and build organisational confidence over time.
5. **GIS Data Management and Retention**
   Strengthen governance over GIS data, including retention practices, ownership, and backup alignment, particularly given its reliance on external platforms and shared services.
6. **Cyber Recovery**
   Ensure cyber incident scenarios are explicitly embedded within IT Disaster Recovery planning, including ransomware, data corruption, and cloud service disruption, with clear linkage to a Cyber Incident Response Plan and wider incident response arrangements.

1 Executive summary

Work Undertaken

In line with each objective, we undertook the following work:

Objective 1: The Organisation has a current and documented IT Disaster Recovery approach appropriate to its systems, services, and operational needs.

- We discussed with the IT team the current approach to IT Disaster Recovery, including how recovery arrangements are understood and applied in practice across the Organisation.
- We reviewed any existing historical documentation and informal materials relating to Disaster Recovery to assess whether these remain relevant to the current hybrid IT environment.
- We considered the extent to which DR arrangements reflect current infrastructure, including cloud-based services, on-premise systems, and third-party platforms.
- We assessed whether there is a consolidated and documented IT Disaster Recovery framework in place that provides a usable and current reference during an incident.

Objective 2: Roles and responsibilities for IT recovery are clearly defined, communicated, and understood by relevant staff.

- We held discussions with a range of stakeholders including the Head of Finance and Corporate Operations, Digital Products Coordinator, Peatland ACTION Programme Manager, GIS Officer, Planning Systems representatives, Information Manager, and IT function representatives.
- We engaged with the IT Service Manager, Systems Engineer, and IT Support Technician to understand operational roles in relation to recovery and incident response.
- We considered how roles and responsibilities are understood in practice across both IT and business functions.
- We reviewed supporting governance materials, including IT policies, acceptable use, information security, and SharePoint ownership arrangements.

1 Executive summary

Objective 3: Critical IT systems, including cloud-based SaaS, on premises systems, and specialist platforms such as Geographic Information System (GIS), are identified and included in recovery planning.

- We discussed key systems in use across the Organisation, including Microsoft 365, IDOX, GIS platforms, and other operational applications.
- We considered how system criticality is understood across both IT and service areas, and whether this is formally documented.
- We reviewed evidence of system information held across SharePoint and other repositories, including third-party system listings and platform ownership details.
- We assessed whether critical systems are mapped to recovery priorities and included within structured Disaster Recovery planning.
- We considered specialist systems such as GIS in relation to data management, dependencies, and recovery considerations.

Objective 4: Backup arrangements are sufficient, reliable, and aligned with operational requirements, including clarity over third-party responsibilities.

- We discussed current backup arrangements across cloud and on-premise environments, including Microsoft 365, file systems, and server infrastructure.
- We reviewed the use of third-party backup solutions, including Metallic, in relation to Microsoft 365 services.
- We considered recent infrastructure changes, including migration from VMware to Hyper-V and implementation of failover capability between sites.
- We assessed the extent to which backup responsibilities are defined between internal teams and external service providers.
- We considered whether there is a consolidated understanding of backup coverage across all systems, including SaaS and third-party platforms.

Objective 5: Recovery expectations, including Recovery Time Objectives and Recovery Point Objectives, are established and aligned to business priorities.

- We discussed organisational understanding of system prioritisation and recovery expectations in the event of disruption.
- We considered whether Recovery Time Objectives and Recovery Point Objectives are formally defined, documented, and aligned to operational and statutory priorities.

1 Executive summary

- We considered how third-party platforms define recovery commitments and whether these are aligned with internal expectations.

Objective 6: Resilience and mitigation measures are in place to reduce the likelihood and impact of IT service disruption.

- We discussed current resilience measures including Microsoft Intune, Microsoft Defender, and endpoint security controls.
- We considered infrastructure resilience, including Hyper-V failover arrangements and hybrid cloud architecture.
- We considered the extent to which IT resilience is aligned with broader organisational continuity arrangements.

Objective 7: Testing on recovery arrangements can be carried out in a proportionate and pragmatic way, with lessons from tests and past incidents applied to strengthen plans.

- We discussed current approaches to testing IT Disaster Recovery arrangements, including any informal or ad hoc recovery activity.
- We considered whether structured testing, scenario-based exercises, or tabletop activities are in place.
- We considered proportionate approaches to testing, including low-risk scenario-based exercises to build organisational understanding and confidence.

Objective 8: IT Disaster Recovery planning considers cyber-related incidents, including the ability to respond to ransomware, data corruption, or cloud service disruption, and that mitigation and recovery measures are appropriate.

- We reviewed cyber security arrangements, including supporting technical controls.
- We considered the use of Microsoft Defender, Intune, and endpoint protection tools in supporting cyber resilience.
- We discussed how cyber incidents would be managed in relation to IT Disaster Recovery arrangements.
- We assessed whether cyber incident response arrangements are formally integrated with Disaster Recovery planning.

1 Executive summary

Conclusion

Conclusion and Summary of Recommendations to Improve Controls

Findings:
This was an advisory review covering the Organisation's IT Disaster Recovery arrangements, including associated documentation, operational practices, and supporting controls. The review focused on current recovery capability across key systems and services, including cloud-based platforms, on-premise infrastructure, and third-party dependencies, with a view to identifying practical and proportionate opportunities to strengthen resilience. As part of this review, we have highlighted areas of good practice currently in place across the Organisation. We have also raised six Action Points to consider, designed to support the further development and formalisation of IT Disaster Recovery and resilience arrangements. Please see **Section 2: Actions Points** to Consider for further information. In addition, we have raised two observations reflecting broader themes and considerations identified during discussions, which may support the continued maturity of the organisation's approach to IT resilience. Please see **Section 3: Observations** for further information.

1 Executive summary

Areas of good practice

The following is a list of areas where the Organisation is operating effectively and following good practice.	
1.	A suite of IT policies is in place, including acceptable use, access management, and administrative account controls, supported by structured SharePoint site ownership and external sharing guidance.
2.	A third-party information management logging system is in place, providing visibility of system activity and supporting auditability of key actions. This enhances oversight of information handling and external interactions across the environment.
3.	Microsoft Intune is in use with defined device policies and compliance controls in place, supported by monitoring and reporting capabilities. This is further complemented by Microsoft Defender and Microsoft 365 security capabilities, including antivirus and endpoint detection and response functionality, which together provide an established baseline for endpoint security and device management across the Organisation.
4.	The Organisation is moving towards more structured security practices, including greater adoption of least privilege principles and improved management of user access across systems. This reflects a positive trajectory in strengthening baseline security controls within a complex environment.
5.	The use of shared service arrangements, particularly in relation to GIS and planning systems, provides access to specialist capability and infrastructure that would be difficult to replicate internally. These arrangements support operational continuity and reflect a pragmatic approach to service delivery at organisational scale.

1 Executive summary

The following is a list of areas where the Organisation is operating effectively and following good practice.	
6.	The Organisation has successfully transitioned a number of services into cloud-based or hybrid environments, including M365 and externally hosted applications.

2 Action points

IT Disaster Recovery Framework and Documentation		
Ref.	Finding and Risk	Recommendation
1.	A clearly defined and accessible IT Disaster Recovery (DR) framework is a key component of organisational resilience, providing a structured approach to restoring systems and services following disruption. As reliance on digital systems, cloud services, and shared platforms continues to increase, having a documented and coordinated approach becomes increasingly important to ensure continuity of operations and minimise service impact. Discussions with the IT team indicated that there is a strong working knowledge of the Organisation's systems and how recovery activities would be approached in practice. This includes an understanding of key infrastructure, dependencies, and potential recovery pathways, particularly in relation to core services such as M365, GIS, and shared systems with external providers. However, this knowledge is largely held within the team and is not formally documented or centrally	We recommend that the Organisation considers developing a concise and practical IT Disaster Recovery document that reflects its current environment. This should outline key systems and dependencies, high-level recovery steps, roles and responsibilities, and key internal and external contacts, including third-party providers. The document should be designed to support use during an incident, with a focus on clarity and usability rather than excessive technical detail, and should be stored in a location that is accessible in the event of system disruption. Consideration should also be given to establishing a periodic review process to ensure the document remains aligned to changes in systems, infrastructure, and operating arrangements over time.

	maintained. A previous IT Disaster Recovery plan was referenced, although this is now considered outdated and does not reflect the current environment, including changes in infrastructure, the transition to cloud-based services, and evolving third-party dependencies. As a result, recovery processes, roles, and key contacts are not clearly captured in a format that could be easily followed during an incident. Our assessment of the root cause is that IT Disaster Recovery arrangements have developed organically over time in response to operational needs, with reliance placed on the experience and knowledge of key individuals. As the Organisation's technology landscape has evolved, including increased complexity and external dependencies, the formalisation of these arrangements into a structured and maintained framework has not kept pace. In the event of a significant incident, the absence of a documented and accessible DR framework may lead to delays in decision-making, reduced clarity over roles and responsibilities, and an increased reliance on key individuals. This may be particularly	

2 Action points

	challenging where incidents occur outside of normal working conditions, involve multiple systems or third parties, or where key staff are unavailable. In addition, without a documented baseline, it may be more difficult to ensure consistency in recovery activities or to incorporate lessons learned from incidents or testing.	

Management response	Responsibility and implementation date
Recommendation agreed Development of a clear and concise plan and the codification of this into a disaster recovery document would assist the team in the responding to an incident. We support the focus of the recommendation on clarity and usability. We will ensure that both digital and hard copies of the plan are stored in locations that are accessible in the event of system disruption. We will also establish a process of periodic review to ensure the document remains aligned to changes in systems, infrastructure, and operating arrangements over time.	*Responsible Officer:* Sandy Allan IT Service Manager *Implementation Date:* December 2026

2 Action points

System Criticality, Prioritisation and Recovery Expectations		
Ref.	Finding and Risk	Recommendation
2.	A clear understanding of which systems are most critical to operations, alongside defined recovery expectations, is fundamental to effective IT Disaster Recovery planning. Establishing priorities and setting realistic expectations for system recovery helps ensure that resources are focused appropriately during an incident and that business needs are aligned with IT recovery capabilities. Discussions with stakeholders indicated that there is a general awareness of which systems are important to the Organisation, particularly in relation to core services such as M365, planning systems (including IDOX), and GIS platforms. It was noted that certain services, such as planning systems, are statutory in nature and would require prioritisation in a disruption scenario. However, this understanding is largely informal and has not been formally documented or consistently agreed across the Organisation. There is currently no defined prioritisation of systems or	We recommend that the Organisation considers defining a simple and proportionate approach to system criticality and recovery expectations. This could include developing a high-level inventory of key systems, supported by a basic prioritisation model, for example categorising systems as critical, important, or non-critical. In parallel, indicative recovery expectations should be established, including how quickly systems should be restored and what level of data loss would be acceptable, with input from relevant business stakeholders. This does not need to be overly detailed, but should provide a clear and shared understanding to support decision-making during an incident and inform wider Disaster Recovery planning.

2 Action points

	services, and recovery expectations, including how quickly systems should be restored or what level of data loss would be acceptable, have not been clearly established. While there is an indication that next business day recovery may be acceptable in some cases, this has not been formally validated with business stakeholders or considered across all systems. Our assessment of the root cause is that system criticality and recovery expectations have not been formally defined as part of a structured IT Disaster Recovery process, with reliance placed instead on operational judgement and implicit understanding. As the organisation's reliance on digital systems has increased, the need for a more structured and agreed approach has become more pronounced. In the event of an incident, the absence of clearly defined system priorities and recovery expectations may result in uncertainty around which systems should be restored first, potentially leading to inefficient use of resources and delays in restoring key services. In addition, without agreed expectations, there is a risk of misalignment between business	

2 Action points

	needs and IT response, which may lead to disruption lasting longer than anticipated or impacting critical services.	

Management response	Responsibility and implementation date
Recommendation agreed We will prepare an inventory of systems and review this with colleagues in the wider organisation to identify priorities. We will also establish indicative recovery expectations, including how quickly systems should be restored and what level of data loss would be acceptable to stakeholders. However, given the separation of finance, HR, payroll and planning software and the website, all hosted externally, it may be there is no requirement to segment the recovery.	*Responsible Officer:* Sandy Allan IT Service Manager *Implementation Date:* October 2026

2 Action points

Backup Arrangements and Third-Party Assurance		
Ref.	Finding and Risk	Recommendation
3.	Effective backup arrangements are a core component of IT Disaster Recovery, providing the foundation for restoring systems and data following an incident. The robustness, coverage, and recoverability of backups are particularly important in environments where services are increasingly distributed across cloud platforms, on-premise infrastructure, and third-party providers. Discussions indicated that backup arrangements exist across a range of systems, however these are varied in approach and maturity depending on the platform and hosting model. Cloud-based services, such as M365, are supported through third-party tooling (e.g. Metallic), while on-premise and legacy environments continue to rely on local infrastructure arrangements, including virtualised environments and storage solutions. It was also noted that certain systems, including GIS and key applications hosted or supported by external partners such as Loch	We recommend that the Organisation considers reviewing and consolidating its understanding of backup arrangements across all key systems, with a view to establishing a clear and documented overview of coverage, responsibility, and recovery capability. This should include clarification of which systems are backed up internally versus those managed by third parties, along with the associated recovery commitments and testing arrangements. Consideration should also be given to introducing periodic test restore activities to provide assurance over recoverability in practice, particularly for critical systems and datasets. In addition, where services are provided by external partners, it would be beneficial to obtain formal assurance regarding their backup and recovery arrangements to support a more complete view of organisational resilience.

2 Action points

	Lomond and IDOX, involve shared or externally managed backup responsibilities. While there is an understanding within the IT team of where backups exist, this is not consistently documented in a single consolidated view, and there is limited formal clarity over the end-to-end coverage across all systems. Our assessment of the root cause is that backup arrangements have developed in a decentralised manner, reflecting the hybrid nature of the Organisation's infrastructure and the involvement of multiple third-party providers. This has resulted in a situation where backup responsibility is distributed across internal teams and external suppliers, without a single overarching framework or consolidated assurance view of coverage, testing, and recoverability. In the event of a significant disruption, this lack of consolidated visibility may make it difficult to quickly confirm what data and systems are recoverable, particularly where responsibilities are shared with third parties. There is also a risk that assumptions are made regarding backup coverage, especially within cloud-hosted or externally managed systems, which may not	

2 Action points

	fully reflect the actual recovery capability. Without regular validation, there is also an increased risk that backups may not perform as expected when required.	

Management response	Responsibility and implementation date
Recommendation agreed We will review and consolidate our understanding of backup arrangements across all key systems, and establish a clear and documented overview of coverage, responsibility, and recovery capability for both internally and externally managed systems. We consider the risk associated with externally managed systems is low, given the size and maturity of the organisations involved (The Access Group, BT, IDOX). Nevertheless, we will request formal assurance over backup and recovery arrangements from all third-party providers. We understand the need for a complete view of organisational resilience. Backup to on premises Commvault has now ceased and is consolidated in Metallic (third-party tool); within a couple of months there will be no requirement to access Commvault. Servers, files on file share, and all 365 data is now on the cloud in Metallic. We will establish a programme of testing the recovery of systems and data.	*Responsible Officer:* Sandy Allan IT Service Manager *Implementation Date:* December 2026

2 Action points

Testing and Exercising of IT Disaster Recovery Arrangements		
Ref.	Finding and Risk	Recommendation
4.	Disaster Recovery arrangements are most effective when they are periodically tested and validated in practice, providing assurance that documented processes and technical capabilities operate as intended. As organisations mature their resilience approach, testing plays a key role in building confidence, identifying gaps, and improving coordination across teams and systems. Discussions indicated that formal testing of IT Disaster Recovery arrangements has been limited to date, with little evidence of structured exercises or regular validation of recovery capability. While there is a practical understanding within the IT team of how systems would be recovered in the event of an incident, this has not been routinely tested through scenario-based exercises or technical recovery simulations. As a result, confidence in recovery arrangements is based largely on knowledge and experience rather than tested outcomes.	We recommend that the Organisation considers introducing a proportionate approach to testing IT Disaster Recovery arrangements. This could include simple scenario-based exercises, tabletop discussions, or targeted recovery tests for key systems. The focus should be on practical validation rather than full-scale simulation, with lessons learned captured and used to improve arrangements over time. Establishing a light but regular testing approach would help build confidence in recovery capability and support the ongoing maturity of the Organisation's resilience framework.

2 Action points

	Our assessment of the root cause is that Disaster Recovery testing has not yet been established as a formal and recurring activity within the organisation's IT resilience approach. As a result, focus has been placed primarily on maintaining operational recovery knowledge and infrastructure, rather than validating end-to-end recovery performance through structured exercises. In the event of a significant incident, the absence of regular testing may mean that recovery processes have not been fully validated under realistic conditions. This could increase the risk of delays, coordination challenges, or unexpected issues arising during recovery, particularly where multiple systems or teams are involved. It may also limit the Organisation's ability to identify and address weaknesses in recovery arrangements before they are exposed in a live incident.	

2 Action points

Management response	Responsibility and implementation date
Recommendation agreed We agree that establishing a light, regular testing approach would help build confidence in recovery capability and support the ongoing maturity of the Organisation's resilience framework. We will start by discussing simple scenarios and build further complexity into our approach as confidence develops within the team.	*Responsible Officer:* Sandy Allan IT Service Manager *Implementation Date:* Discussion of simple scenarios over the next six months (to November 2026). Plan developed for more complex testing by March 2027.

2 Action points

GIS Data Management and Retention		
Ref.	Finding and Risk	Recommendation
5.	Effective management and retention of GIS data is an important consideration given its role in supporting operational delivery, planning activities, and evidence-based decision making across the Organisation. The integrity, structure, and availability of GIS datasets directly impact the Organisation's ability to access spatial information in both business-as-usual and recovery scenarios. Discussions with the GIS function indicated that GIS is a critical tool used across a range of activities, with reliance on both internally managed data and datasets held or supported through external arrangements, particularly with shared service partners. It was noted that GIS data is used for operational delivery, planning support, and reporting purposes, and in some cases is dependent on connectivity to external environments or services. While key datasets are understood by users in practice, there is limited formal classification or documented retention framework in place to	We recommend that the Organisation considers reviewing its GIS data management and retention arrangements with a view to introducing a more structured and proportionate approach. This could include defining key datasets, establishing clear ownership and accountability, and introducing basic retention principles to ensure that critical spatial data is appropriately managed throughout its lifecycle. Consideration should also be given to rationalising existing data structures where appropriate, reducing duplication, and improving clarity over authoritative data sources. This approach would help strengthen data resilience, improve consistency, and support more effective recovery and continuity in the event of disruption.

	consistently define what data is critical, how long it should be retained, and where authoritative versions should reside. In addition, the current environment includes a degree of legacy structure and historical data accumulation, which has contributed to inconsistency in how data is stored, accessed, and maintained over time. Our assessment of the root cause is that GIS data management and retention arrangements have evolved organically alongside operational use of the system, with a strong focus on usability and access rather than formal data governance and lifecycle management. As a result, structured retention rules, ownership definitions, and standardised data management practices have not been fully established or consistently applied. In the event of data loss, system disruption, or the need to recover from an incident, the absence of clearly defined retention arrangements and structured data governance may make it more difficult to determine authoritative datasets, prioritise recovery of critical information, or ensure consistency in restored data. This may be further complicated	

2 Action points

	by the presence of duplicated or legacy datasets, where it is not always clear which version should be treated as the definitive source.	

Management response	Responsibility and implementation date
Recommendation accepted. This is a long-standing issue, which the organisation is seeking to resolve. GI Data classification / management work is already ongoing, in two parallel streams (Peatland ACTION and other). Recruitment of information management intern in second half of 2027 will accelerate progress. There needs to be organisational agreement over structured retention rules, ownership definitions, and standardised data management practices.	*Responsible Officer:* Information Manager in collaboration with the IT Service Manager. *Implementation Date:* 31 March 2027

2 Action points

Cyber Recovery		
Ref.	Finding and Risk	Recommendation
6.	The integration of cyber resilience into IT Disaster Recovery planning is increasingly important as organisations face a growing range of threats, including ransomware, data corruption, and targeted attacks. Effective recovery planning in this context requires not only the ability to restore systems, but also confidence that systems and data can be restored to a known good state following a cyber incident. Discussions indicated that cyber security controls are in place across the Organisation, including endpoint protection and cloud-based security tooling, and there is general awareness within the IT team of the need to consider cyber-related scenarios. However, there is currently no formal Cyber Incident Response Plan (CIRP) in place. As a result, the Organisation does not have a clearly defined or documented approach for how it would respond to and manage a cyber incident in a structured and coordinated manner. In addition, the	We recommend that the Organisation considers developing a formal Cyber Incident Response Plan, setting out how cyber incidents would be identified, escalated, managed, and contained. This should clearly define roles and responsibilities, escalation routes, and coordination with IT Disaster Recovery processes to ensure a joined-up approach to response and recovery.

	linkage between cyber incident response activity and IT Disaster Recovery arrangements is not formally defined, which limits clarity over how recovery would be initiated and managed following a cyber event. Our assessment of the root cause is that cyber incident response has not yet been formalised as a distinct component of the Organisation's wider IT resilience and risk management framework. As a result, while individual technical controls are in place, these have not been brought together into a structured and documented response framework that clearly defines roles, responsibilities, escalation routes, and recovery considerations. In the event of a cyber incident, the absence of a formal CIRP may result in uncertainty around how the Organisation should respond, particularly in the early stages of an incident where containment and recovery decisions need to be made quickly. This may also impact the ability to coordinate response activities effectively across IT and wider business functions, and could lead to delays or inconsistencies in recovery actions, particularly where system integrity needs to be confirmed	

2 Action points

	prior to restoration.	

Management response	Responsibility and implementation date
Recommendation agreed We will developing a documented Cyber Incident Response Plan, setting out how cyber incidents would be identified, escalated, managed and contained, and which defines roles and responsibilities, escalation routes, and coordination with IT Disaster Recovery processes. We have obtained CISP cyber response playbooks and will embedded these in our recovery procedures.	*Responsible Officer:* Sandy Allan IT Service Manager *Implementation Date:* March 2027

3 Observations

The following is a list of observations from our review	
1.	The IT function operates within a small team supporting a wide and increasingly diverse digital environment, with a mixture of internally managed systems and externally supported services. This reflects a common operating model in organisations of this type, where reliance on shared services and third-party providers plays an important role in delivering core infrastructure and applications. As the Organisation continues to evolve digitally, this model presents both benefits and considerations. On the one hand, it enables access to specialist capability and supports operational delivery across a broad system landscape. On the other, it introduces a level of dependency on external parties and can influence the capacity available for structured development activity, documentation, and longer-term resilience planning. As arrangements mature, maintaining clarity around roles, responsibilities, and dependencies will continue to be important in supporting effective prioritisation and ensuring that resilience improvements can be progressed in a sustainable way.
2.	Discussions indicated that there is an emerging understanding of the relationship between Business Continuity and IT Disaster Recovery, with both areas broadly recognised as being connected in supporting organisational resilience. As arrangements continue to mature, there is an opportunity to further strengthen the alignment between business-facing continuity planning and IT recovery capabilities. At present, the linkage between the two areas appears to be largely based on operational understanding and informal coordination, rather than a fully documented and consistently applied framework. In practice, this means that expectations around recovery timeframes and service restoration may be understood at a high level, but are not always formally defined or consistently communicated across all stakeholders. As the Organisation continues to develop its resilience approach, there would be benefit in maintaining and building on this alignment to ensure that business priorities and IT recovery planning remain closely connected.

4 Audit arrangements

The table below details the actual dates for our fieldwork and the reporting on the audit area under review. The timescales set out below will enable us to present our final report at the next Audit & Risk Committee meeting.

Audit stage	Date
Fieldwork start	20 April 2026
Closing meeting	6 May 2026
Draft report issued	8 May 2026
Receipt of management responses	27 May 2026
Final report issued	29 May 2026
Audit & Risk Committee	19 June 2026
Number of audit days	8

6 Key personnel

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
Senior	Shaun Roddan	Senior IT Auditor	srr@wbg.co.uk

Cairngorms National Park Authority			
Key Contacts:	Louise Allen	Head of Finance & Corporate Operations	louiseallen@cairngorms.co.uk
	Daisy Whytock	Peatland ACTION Programme Manager	daisywhytock@cairngorms.co.uk
	Sandy Allan	IT Service Manager	sandyallan@cairngorms.co.uk
	Paul Davison	Information Manager	pauldavison@cairngorms.co.uk

6 Key personnel

	Adam Alexander	Digital Projects Coordinator	adamalexander@cairngorms.co.uk
	Deirdre Straw	Planning Systems Officer	deirdrestraw@cairngorms.co.uk
	Andy Smith	GIS Officer	andysmith@cairngorms.co.uk
	Sally Newton	GIS Manager (Loch Lomond & Trossachs National Park)	sally.newton@lochlomond-trossachs.org
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.			

Appendices

1 Potential key risks

Purpose of review

The purpose of this advisory review is to assess Cairngorms National Park Authority's (the Organisation's) IT Disaster Recovery arrangements in the context of current hybrid working, cloud-based services, and recent digitisation. The review will focus on the practical effectiveness of recovery planning, supporting documentation, and mitigation measures, providing pragmatic recommendations to strengthen IT resilience going forward.

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

Scope of review

Our objectives for this review are to review and advise on the Park Authority's IT Disaster Recovery arrangements, supporting the development of proportionate processes and documentation aligned to its systems, services, and operational requirements. Our objectives for this review are as follows:

- The Organisation has a current and documented IT Disaster Recovery approach appropriate to its systems, services, and operational needs.
- Roles and responsibilities for IT recovery are clearly defined, communicated, and understood by relevant staff.
- Critical IT systems, including cloud-based SaaS, on premises systems, and specialist platforms such as Geographic information system (GIS), are identified and included in recovery planning.
- Backup arrangements are sufficient, reliable, and aligned with operational requirements, including clarity over third-party responsibilities.
- Recovery expectations, including Recovery Time Objectives and Recovery Point Objectives, are established and aligned to business priorities.

1 Potential key risks

- Resilience and mitigation measures are in place to reduce the likelihood and impact of IT service disruption.
- Testing on recovery arrangements can be carried out in a proportionate and pragmatic way, with lessons from tests and past incidents applied to strengthen plans.
- IT Disaster Recovery planning considers cyber-related incidents, including the ability to respond to ransomware, data corruption, or cloud service disruption, and that mitigation and recovery measures are appropriate.

We will also:

- Consider the organisation's IT Team's understanding of their approach to disaster recovery, and associated operational arrangements in place, including arrangements shared with Loch Lomond and the Trossachs National Park Authority, and whether there are control gaps in these practices.
- Consider whether back-up arrangements in place within current operations are sufficient, reliable, and aligned with operational requirements, including clarity over third-party responsibilities.
- Consider the IT team's recovery expectations in the event of any loss of systems.
- Consider the IT team's understanding of resilience and mitigation measures in place or planned to mitigate the impacts of any service disruption
- Consider the organisation's current approach and controls regarding cyber security
- Consider the extent to which the organisation has developed a written IT Disaster Recovery approach documenting these operational arrangements.

1 Potential key risks

Limitation of scope

There is no limitation of scope.

Audit approach

Our approach to this advisory review will be collaborative and forward-looking, focusing on understanding your current IT Disaster Recovery (DR) arrangements, identifying areas for practical enhancement, and supporting the development of proportionate and sustainable recovery capabilities.

Specifically, we will:

- Hold discussions with key personnel to understand the current IT Disaster Recovery arrangements. This will include exploring how DR planning aligns with the Organisation's wider Business Continuity arrangements, how roles and responsibilities operate in practice, and how recovery activities would be coordinated in the event of a disruption.
- Obtain and review information on the Organisation's IT Disaster Recovery framework, including previous DR plans, backup procedures, resilience measures, and records of any previous recovery activities.
- Explore the coverage of critical IT systems and services, including cloud-based SaaS platforms, on-premises infrastructure, GIS, and other key applications. We will discuss how criticality has been determined and whether recovery expectations are clearly articulated and aligned with operational priorities.
- Discuss existing resilience and mitigation features, such as redundancy, failover arrangements, supplier dependencies, and alternative working solutions, to understand how the Organisation currently reduces the likelihood and impact of service disruption.
- Consider suitable pragmatic approaches to exercising and validating IT recovery arrangements, including scenario-based discussions or modular testing.
- Explore how cyber-related scenarios (e.g. ransomware, data corruption, or cloud service disruption) might be considered within IT Disaster Recovery and how these arrangements should best interface with incident response processes.
- Provide advisory observations and practical recommendations to support the enhancement, clarification, and prioritisation of IT recovery and resilience arrangements, recognising the Organisation's size, complexity, and risk appetite.

1 Potential key risks

This review will not include detailed controls testing or formal assurance over the design and operating effectiveness of specific controls. Instead, it will provide insight into current arrangements and identify opportunities for proportionate improvement.

Potential key risks

As this engagement is advisory in nature, we will not present "key risks" in a traditional assurance format. Instead, our work will focus on exploring the following thematic areas:

Clarity and Structure of IT Disaster Recovery Arrangements

Whether there is a clear and usable DR framework that supports structured response and recovery activity.

Roles, Responsibilities and Governance

How accountability and decision-making operate during a disruption, and whether escalation and communication pathways are understood.

Identification and Prioritisation of Critical Systems

How the Organisation determines which systems and services are critical, and how recovery priorities are established.

Backup and Data Recovery Arrangements

The practical arrangements in place to enable restoration of systems and data, and the clarity of recovery expectations.

1 Potential key risks

Resilience and Service Continuity Measures

The extent to which technical and supplier-based resilience measures reduce reliance on reactive recovery.

Exercising and Continuous Improvement

How the Organisation gains assurance that recovery arrangements are workable in practice and how lessons learned inform improvement.

Integration with Cyber and Incident Response

The alignment between IT Disaster Recovery planning and broader cyber or major incident response arrangements.

This advisory review will aim to provide constructive insight into the current maturity of arrangements and highlight pragmatic steps that can strengthen overall IT resilience over time.