For discussion

Title: Internal audit review – IT disaster recovery advisory

Prepared by: Cover paper-Louise Allen, Head of Finance and Corporate Operations

Paper: Shaun Roddan, wbg-assignment leader

Purpose

This paper presents the results of the Internal Auditor's advisory review on IT disaster recovery procedures. The purpose of the review was to assess Park Authority'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.

Recommendations

The Audit and Risk Committee is asked to

a) Consider the internal auditors report and findings.
b) Endorse the management responses to recommendations for future action and improvements.

Executive Summary

1. The aim of the assignment was to provide guidance to the Park Authority, and in particular, to its IT and Information Management teams, to support the development of proportionate processes and documentation, giving confidence that, on completion of the improvements recommended, the following objectives will have been met:

    a) The Organisation has a current and documented IT Disaster Recovery approach appropriate to its systems, services, and operational needs.
    b) Roles and responsibilities for IT recovery are clearly defined, communicated, and understood by relevant staff.

c) 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.
d) Backup arrangements are sufficient, reliable, and aligned with operational requirements, including clarity over third-party responsibilities.
e) Recovery expectations, including Recovery Time Objectives and Recovery Point Objectives, are established and aligned to business priorities.
f) Resilience and mitigation measures are in place to reduce the likelihood and impact of IT service disruption.
g) 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.
h) 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.

2. The report recognises the IT team's 'strong working knowledge of the Park Authority's systems and their understanding of key infrastructure dependencies. It stresses the need for this knowledge to be documented to guide action in the event of a recovery situation.

3. Examples of good practice identified are shown in the table below. It is reassuring to see the progress made in developing our IT systems to greater maturity.

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

4. The Auditor's recommendations are:
   a) the development of a concise and practical IT Disaster Recovery document
   b) definition of a simple and proportionate approach to system criticality and recovery expectations
   c) review and documentation of backup arrangements across all key systems
   d) development of testing protocols
   e) the review of GIS data management and retention arrangements
   f) the documentation of a formal Cyber Incident Response Plan

Conclusion

5. This was a helpful and informative piece of work, carried out in a supportive manner and well received by the teams at the Park Authority. We are grateful to the Auditor for his approach and for the recommendations made.

6. The recommendations made were accepted by management.

Louise Allen
louiseallen@cairngorms.co.uk
03 June 2026