For decision

Title: Update on outstanding internal audit recommendations

Prepared by: David Cameron, Deputy Chief Executive and Director of Corporate Services

Purpose

This paper presents an update on actions underway which address outstanding internal audit recommendations on controls relating to information technology, cyber security and information management. The paper proposes revised, updated actions for adoption by the Committee in place of the existing recommendations which in some cases are outdated following significant action by the Park Authority's teams working in this area.

Recommendations

The Audit and Risk Committee is asked to:

a) Agree the six prior internal audit recommendations set out at 1 are superseded.
b) Agree the adoption of the three actions set out at 6 as replacement actions required to implement an appropriate overarching control environment for the Park Authority's IT and data management operations.
c) Agree to receive updates on progress against these actions as part of updates on action in implementing audit recommendations.
d) Agree the scope of any internal audit work in these areas over the next 12 months should reflect the status of the current evolution of the Park Authority's operating environment for IT and data services.

Background

1. The update on outstanding internal audit recommendations presented to the Audit and Risk Committee at its previous meeting highlighted six of 20 outstanding recommendations that link to the Park Authority's work in the areas of information technology, cyber security and information management. The recommendations are:
   a) 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. [Partially complete]

b) 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. [Partially complete]

c) 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 [Partially complete]

d) 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. [Incomplete]

e) We recommend that CNPA review the current policy suite that is in place and develop and implement policies that address policy areas covering data management and retention; information transfer; cloud security; access control; back up and resilience; data labelling; [Partially complete]

f) 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 [Incomplete]

2. The recommendations above are all inter-related, with information technology infrastructure and approaches influencing data management; and overall information and data strategies linked to risk management and business continuity.

3. The Park Authority has designed and implemented step change developments in its information technology and data management environment over the last couple of years. This has included movement to Microsoft 365 and cloud-based operations; complete overhaul and implementation of records management systems based on SharePoint; evolution and enhancement of our Information Management and GIS systems and team resources; and successful implementation of IT Management actions to secure Cyber Essentials Plus accreditation.

4. This investment, and work by our teams, has made significant progress in addressing a range of control weaknesses highlighted in prior internal audit reports. As noted above, most recommendations have been classified as 'partially complete' with action progressing. Some recommendations have not been progressed as work in these control areas can only begin once we have made a decision on how best to develop our IT and Data Management systems. For example, we need to embed our approaches to both IT use and information management, before redesigning and implementing business continuity plans and actions. The most

appropriate approach to business continuity planning will be determined by how our information is held and backed up, and by the various ways of accessing that information.

5. There are strong links between the Cairngorms IT infrastructure and network and that of Loch Lomond and the Trossachs National Park Authority (LLTNPA) through shared services activities that have now been in place for several years. With evolution of the teams at both Cairngorms and LLTNPA, and significant changes in our operating environments, there is also a need for review and refresh of these shared services arrangements.

Future Action

6. Given the scale of refresh and renewal of the Park Authority's operating environment, we are now in the process of developing a new, strategic overview of our position and establishing an updated long-term direction on our IT and Information Management. The key actions underway to bring the Park Authority to a clear basis for robust, sustainable and secure operations are:
   a) Establish an IT Strategy, encompassing a refreshed understanding of our shared service arrangements with LLTNPA, together with a costed action plan which underpins future delivery of IT and data services. We are working to complete this before the end of the current financial year, 31 March 2026.
   b) Complete our embedding of information management approaches, including GIS and other data management and publication policies, including our statutory records management duties Again, we are working to complete this before the end of the current financial year, 31 March 2026. There is some dependency of this work to completion of the IT Strategy work.
   c) Develop our business continuity plan in the context of the evolving IT Strategy and information management approaches and embed an understanding of the Park Authority's approach to business continuity across the organisation. We expect June 2026 is the earliest feasible deadline for effective completion of this element of work.

7. It seems appropriate to replace the six outstanding internal audit recommendations with the above three actions.

8. Updates on progress against these three actions will be provided to the committee at appropriate intervals, including as part of updates on outstanding audit recommendations.

David Cameron
davidcameron@cairngorms.co.uk
11 June 2025