AZETS

Cairngorms National Park Authority

Internal Audit Report 2021/22

Cyber Security Review

April 2022

Cairngorms National Park Authority

Internal Audit Report 2021/22

Cyber Security Review

Executive Summary 1

Management Action Plan 4

Appendix A – Definitions 8

Audit Sponsor	*Key Contacts*	*Audit team*
David Cameron- Director of Corporate Services	*Sandy Allan- Information Systems Manager* *Daniel Ralph- Finance Manager*	*Paul Kelly- IT Audit Director* *Ashley Bickerstaff- IT Audit Manager* *Dominic O'Neill- IT Auditor* *Natasha Williams- IT Auditor*

Executive Summary

Conclusion

Our review of the CNPA's cyber security risk management found that improvements could be made to enahance the organisations ability to manage and handle cyber related events. The organisation would benefit from etsblishing a more formalised and structured approach to management of lower-level cyber related risks. The organisation would also benefit from formalising the procedures that should be followed when a cyber related event occurs.

Our review has also identified that although cyber security training is in place the completion rate of this is low with 58% of staff completing this.

Background and scope

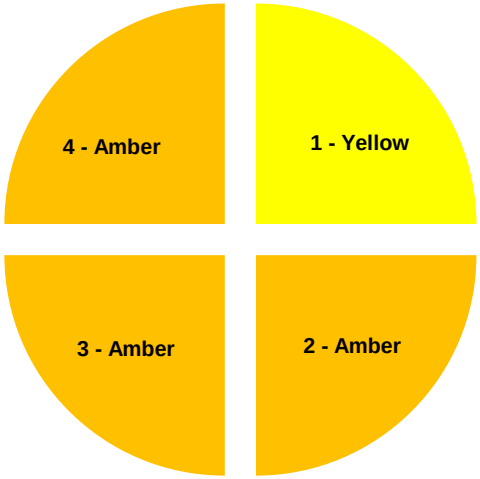
Cyber security represents a significant risk to the majority of public bodies, with the risk having increased during the Covid-19 pandemic.

It is important that organisations have well-defined approaches in place to minimise risks associated with technical, policy and behavioural elements of cyber security.

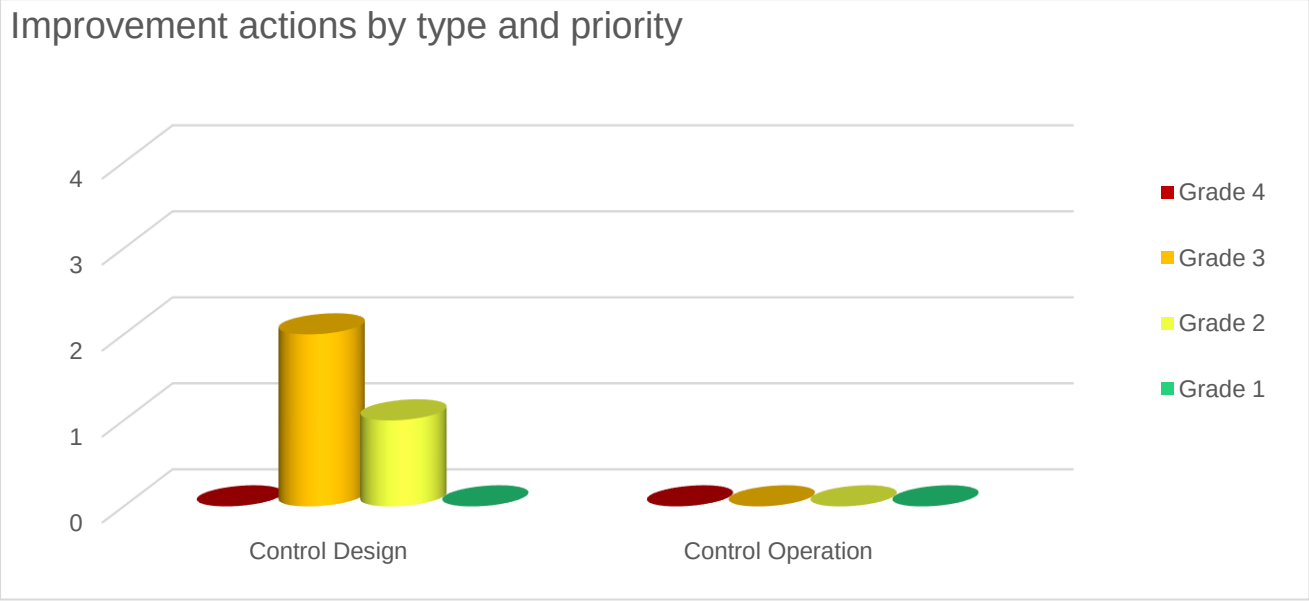
The Cairngorms National Park Authority (CNPA) is going through a significant change process in relation to cyber security with investment in cyber security defences.

Our review has soughtto confirm that the CNPA has adequate measures in place for cyber security and that the strategy for managing cyber security risks is aligned to leading practice.

Control assessment



- 1. There are adequate technical controls in place to protect the corporate network from cyber security threats.
- 2. There is adequate cyber security training and awareness for staff and third parties.
- 3. There are defined process for identification, recording and management of cyber security risks.
- 4. The proposed strategic approach to managing cyber security risk is aligned to leading practice.



Three improvement actions have been identified from this review, all of which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Areas for improvement

We have identified areas for improvement which, if addressed, would strengthen CNPA's control framework. These include:

- There is a reactive approach to managing cyber security risks. There is two high-level cyber related risks on the Strategic Risk Register but there is no lower-level management of cyber-related risks.
- Training in relation to cyber security is in place however completion is low with 58% completing the course.

These are further discussed in the Management Action Plan below.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Management Action Plan

Control Objective 1: There are adequate technical controls in place to protect the corporate network from cyber security threats.

Yellow

1.1 Procedures and testing

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.

Risk

Without tested procedures to handle a cyber event, there is an increased risk of a successful cyber event leading to downtime, reputation and financial damage.

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.

Management Action

Grade 2 (Design)

Recommendation accepted.

Action owner: Information Systsems Manager

Due date: 31 December 2022

Control Objective 2: There is adequate cyber security training and awareness for staff and third parties.

Amber

2.1 Cyber Security Training and Awareness

CNPA has staff cyber security training in place. This makes use of the UK National Parks Electronic Learning Management System (ELMS). As part of the mandatory training courses, cyber security, data security and data protection courses are included.

Completion of the mandatory training courses is low within CNPA. The cyber security training course has 69 active staff enrolled, of which 40 (58%) have completed the course. There is no process established to monitor the completion of the mandatory training courses.

The training is not refreshed, with the cyber security training course launched in February 2018 with no requirement for staff to refresh the training.

We also identified that CNPA has not yet created an ongoing campaign of staff awareness to reinforce the training and to periodically provide updates on risks.

Risk

Without adequate training and awareness there is a risk that staff will not be informed of how to protect themselves and organisations data and systems from a cyber security attack. This may result in organisation data being compromised and significant business disruption. There is also the risk of reputational damage and financial penalty for the organisation.

Recommendation

We recommend that management should update and refresh the mandatory cybersecurity training annually for all staff and that the training should form part of induction training for new staff.

We also recommend that, when training commences, there is regular monitoring of completion rates with appropriate mechanisms for escalation where staff persistently do not complete this.

Management Action

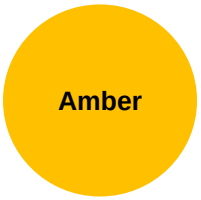
Grade 3 (Design)

We will reinvigorate training and ensure all staff complete the mandatory modules as a matter of priority, monitoring completion rates to ensure compliance. We will also liaise with the training module provider to ensure the training is appropriately and regularly refreshed.

Action owner: Head of Organisational Development **Due date:** 31 August 2022

Control Objective 3: There are defined process for identification, recording and management of cyber security risks.

Control Objective 4: The proposed strategic approach to managing cyber security risk is aligned to leading practice.



3.1 Cyber Risk Managament

Our audit found that CNPA could enhance the cyber risk management practices and that the organisation 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.

Risk

There is the risk that there are no processes in place for identifying, recording and managing cyber security risks. As a result, these risks may manifest more regularly.

There is the risk that the proposed strategic approach to risk management does not align with leading practice and as a result, is not as effective as it should be.

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 the results of these.

Management Action

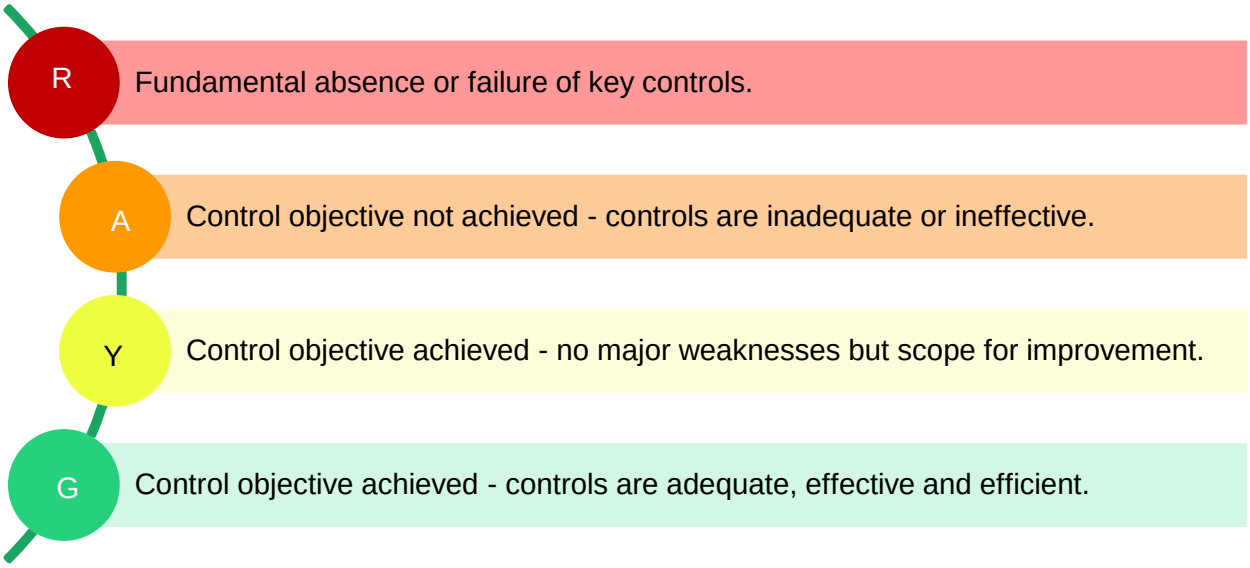
Grade 3 (Design)

We will undertake a risk analysis of cyber risk and establish a mapping of risk against protection provision, with consequent identification of any gaps. We will establish an action plan to address any such gaps arising.

Action owner: Information Systems Manager **Due date:** 31 August 2022

Appendix A – Definitions

Control assessments



Management action grades

4	•Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.
3	•High risk exposure - absence / failure of key controls that create significant risks within the organisation.
2	•Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.
1	•Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.