AUDIT GLASGOW

Loch Lomond and the Trossachs National Park Authority

Cyber Resilience

Final Report

February 2023

Glasgow CITY COUNCIL

bsi ISO 9001 Quality Management Systems CERTIFIED

FS 57095

1 Introduction

1.1 As part of the agreed Internal Audit plan, we have carried out a review of Cyber Resilience at the Loch Lomond and the Trossachs National Parks Authority (LLTNPA).

1.2 LLTNPA aims to protect and preserve the natural and cultural heritage of the park, which encompasses around 720 sq. miles across a range of terrains, including of mountains, lochs and rivers. LLTNPA has around 180 permanent and seasonal staff, and whilst the majority use PCs as part of their day-to-day work, there are some sections, e.g., park rangers, who are predominantly out in the field.

1.3 Cyber-attacks can take many forms (e.g., ransomware, business email compromise, denial of service etc.) and security experts suggest that it is generally a case of when and not if one will occur. There have been some high-profile cyber incidents within the Scottish public sector in recent years, which have had a significant impact on their ability to deliver services.

1.4 It is therefore essential that organisations adopt a cyber resilient approach, which focuses on protecting core services and preventing issues before they occur. This can involve identifying the risks and vulnerabilities, associated with the services that support critical business processes, and managing these effectively. And whilst every effort is made to prevent IT / cyber security incidents it is essential that organisations can respond effectively to them, should they occur.

1.5 The purpose of this audit was to obtain assurance that LLTNPA has the appropriate processes in place for identifying and managing information security (IS) / cyber related risks, before they crystallise, and has the means to respond effectively when they do.

1.6 The scope of the audit included an assessment of:

- Cyber awareness training and communications.
- Horizon scanning and threat intelligence processes.
- Risk and vulnerability management arrangements.
- Back-up and recovery processes.
- Incident response management arrangements.

2 Audit Opinion

2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and 5 recommendations which management should address.

3 Main Findings

3.1 We are pleased to report that the majority of key controls are in place and generally operating effectively. We found that LLTNPA has successfully obtained the Cyber Essentials Plus (CE+) certification that this had been re-confirmed within the last 12 months.

3.2 Both ICT and Information Security (IS) Policies were found to have been in place and these are readily accessible to all staff via the authority's intranet, ParkCentral.

3.3 We found that there are a number of cyber-related training courses available to staff via the ELMs HR system and the recently adopted Boxphish tool, which simulates phishing based attacks and educates staff via post simulation training. Furthermore, we found that training is supplemented through ad hoc staff communications, as and when cyber security alerts / threats arise.

3.4 Network traffic is continuously monitored via an artificial intelligence driven tool which is capable of identifying anomalous behaviour. Twice monthly vulnerability scanning also takes place and vulnerabilities are logged and prioritised appropriately. The ICT Manager is a member of the Cyber Security Information Sharing Partnership (CISP) and LLTNPA makes use of the active cyber defence services made available by the National Cyber Security Centre (NCSC). A currency roadmap has also been developed to identify and manage systems which are going out of support, before they become a security vulnerability.

3.5 Cyber risk is included in the organisational risk register and is reported to the Board on a routine basis.

3.6 We confirmed that data is routinely backed up with copies taken across multiple media types and we were advised that data back-ups are securely stored offsite. This helps to minimise the risk of significant data loss during a cyber incident, e.g., ransomware attack.

3.7 An IT Disaster Recovery (DR) Plan has been developed to support the technological aspects of the Business Continuity Plan (BCP).

3.8 However, our audit testing found that there are some opportunities for improvement.

3.9 The policy review arrangements were not documented, and it is unclear when the ICT Policy was last reviewed with various dates ranging from May 2018 to January 2020 noted in the document. It is acknowledged however that LLTNPA had already identified the policy review requirements and these are included on the IS workplan, to be addressed during 2023. As such no further recommendation has been made.

3.10 Whilst we were advised that a training compliance target of 80% had been set (i.e., staff must have completed at least 80% of the monthly Boxphish courses available), we found that 45 (25%) employees were not achieving this, with 16 (9%) having completed 0 of the 9 courses available at the time of the audit fieldwork. We have been advised that some factors, outwith the control of LLTNPA (e.g. long-term sickness absence. maternity leave etc.), have also had an impact on training compliance levels

3.11 The current vulnerability log used by LLTNPA to track and respond to known vulnerabilities could be further enhanced. The log currently only lists vulnerabilities identified through scanning and does not include external threat intelligence sources, e.g., NCSC or CISP. Vulnerabilities have not been assigned ownership and it is unclear who is responsible to managing the associated risk.

3.12 More widely cyber risk is currently only documented at a high level, with a single overarching risk noted in the organisational risk register. However cyber-attacks vary significantly and as a result the mitigations for managing each cyber risk also vary.

3.13 Although data back-ups were being taken successfully, we found that LLTNPA does not currently undertake restoration testing to assess the effectiveness of back up processes. Similarly, although a DR plan is in place this has not been reviewed in 2 years or formally tested in around 4 or 5 years.

3.14 A high-level Cyber Incident Response Plan has been developed using the Scottish Government's templates however this was still in draft and had not been approved for use. Detailed scenario-based playbooks had not been developed at the time of the fieldwork, though we noted that there are plans for these to be created in 2023 as part of the IS workplan. No further recommendation has been made in light of this.

3.15 An action plan is provided at section four outlining our observations, risks and recommendations. We have made 5 recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	0
Medium	Less critically important controls absent, not being operated as designed or could be improved.	3
Low	Lower level controls absent, not being operated as designed or could be improved.	2
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

3.16 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.17 We would like to thank officers involved in this audit for their cooperation and assistance.

3.18 It is recommended that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Staff are adequately trained and compliance is monitored and escalated as necessary.				
1	LLTNPA currently train staff in cyber security using two systems. Traditionally training has been delivered via the ELMs HR training system however, more recently, phishing simulations and training have been delivered via the Boxphish tool, which was launched in early 2022. The IT Manager advised that staff are required to complete at least 80% of the monthly training courses issued by the Boxphish system. However, on review we found that of the 180 staff listed on the training report 45 (25%) had not achieved the compliance target. A subsection of this - mostly rangers - had not completed any of the courses available. Compliance reports are currently issued to operational managers on a two monthly basis and persistent non-compliance is escalated to the Director of Corporate Services. The arrangements for raising compliance levels however are not operating effectively, therefore there is an increased risk that staff do not identify potential	LLTNPA management should review the arrangements for managing training compliance and determine whether it is possible to implement stricter compliance mechanisms, e.g. LLTNPA may wish to consider: • More regular senior management reporting. • The development of implementation plans to track progress etc.	**Medium**	**Response:** Accepted Proposed compliance procedure: • Maximum of two non-completed training modules at time of reporting • Reports sent to managers every 2 months, ○ It is the mangers responsibility to ensure that staff are completing the training and adhering to the IS Security Policy • Repeat offenders (those who appear multiple times as being non-compliant) ○ The offender and their manager will receive an email with a 1-week deadline for the training modules to be complete. ○ Failure to complete will see the matter escalated to their Director and/or system access revoked.

No.	Observation and Risk	Recommendation	Priority	Management Response
	cyber threats before they occur or know how to respond to them when they do.			**Officer Responsible for Implementation:** IS Manager **Timescales for Implementation:** Complete

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Cyber related threats, vulnerabilities and risks are recorded, assessed and managed in line with their priority.				
2	A vulnerability log has been developed and this is populated with the outputs from the periodic vulnerability scans that run. A log of threats from other sources (e.g., NCSC, Scottish Government, CISP etc.) however is not currently maintained. Furthermore. we found that vulnerabilities are not currently assigned to named individuals for remediation. A name and date are only added following resolution. As such it is unclear who is responsible for managing each vulnerability. There is therefore an increased risk that threats and vulnerabilities not recorded or managed and could become exploited.	The IT Manager should further develop the vulnerability log so that threat alerts from other sources are recorded. Each log entry should also be assigned to a named owner, responsible for its management.	**Low**	**Response:** Accepted Relevant vulnerabilities have, and will continue to be, added to the log. Log has now been updated and each vulnerability will be assigned an owner. **Officer Responsible for Implementation:** IS Manager **Timescales for Implementation:** Complete
3	A single, high-level cyber risk is recorded on the Corporate Risk Register, along with a series of mitigating actions and this is reported to the LLTNPA Board as required. However. there is currently no operational IT / Cyber Risks Register in place for recording and managing the various cyber related threats that LLTNPA may encounter.	LLTNPA management should develop an IT Risk Register, which includes the range of cyber-related risks that the organisation may encounter. Risks should be appropriately recorded and assessed, with suitable mitigations applied to reduce the likelihood and/or impact of the risk. Risks should be assigned to named owners and reported and escalated as necessary.	**Medium**	**Response:** Accepted LLTNPA will implement an IT Risk Register in line with the Risk Management Framework and escalation trigger points. **Officer Responsible for Implementation:** IS Manager **Timescales for Implementation:** 31 December 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Back-up and recovery testing is undertaken on a regular basis.				
4	We were informed by the IT Manager that a project is underway for back-up and DR processes to be migrated to a cloud solution in 2023. This should increase resilience while simplifying back-up and recovery processes and reducing reliance on manual tape back-ups. As a result of this project, we were advised however that back-up and recovery documentation (e.g. the DR Plan) has not been reviewed in 2 years. Furthermore, although we found examples which show that backed up data can be restored upon request, a formal back-up and recovery test has not taken place for up to 5 years. Without up to date and tested back-up and recovery plans there is an increased risk that LLTNPA is unable to recover to a suitable state following cyber incident.	The IT Manager should ensure that back-up and DR plans are reviewed and updated to reflect the back-up and recovery environment. The DR plan should be kept under regular (e.g., annual) review thereafter. Once the back-up and recovery documentation has been updated appropriate testing should be undertaken to assess the effectiveness of the Plans in place.	**Medium**	**Response:** Accepted. Given the delays to the Cloud DR implementation, and as an outstanding item on the IT General Controls audit, the DR Plan will be updated and tested. This will be repeated when the Cloud DR solution goes live. **Officer Responsible for Implementation:** IS Manager **Timescales for Implementation:** 31 March 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: A Cyber Incident Response Plan has been documented and approved.				
5	We were advised that a review of the SEPA action plan was undertaken at the time of release, however no formal gap analysis was conducted to assess LLTNPA's position in relation to each of the actions. As such there is an increased risk that key outcomes have not been identified and threat actors exploit security gaps.	LLTNPA management should consider whether a formal gap analysis should be conducted to assess the authority's position in relation to each action. Where gaps are identified appropriate plans should be put in place to improve LLTNPAs position in relation to these.	**Low**	**Response:** LLTNPA have considered the requirements for a gap analysis to be undertaken but feel that this would not add value due to the passage of time since the incident. This will, however, be considered for future incidents affecting partner organisation, where details of the event are made public. **Officer Responsible for Implementation:** IS Manager **Timescales for Implementation:** Complete