Comhairle nan Eilean Siar
Internal Audit Follow Up Review
Cyber Attack Response
Final Report – FU08-24/25

14 January 2025

COMHAIRLE NAN EILEAN SIAR
INTERNAL AUDIT FOLLOW UP REPORT
CYBER ATTACK REPSONSE

CONTENTS

COMHAIRLE NAN EILEAN SIAR
INTERNAL AUDIT FOLLOW UP REPORT
CYBER ATTACK REPSONSE

SECTION 1: EXECUTIVE SUMMARY

Introduction

1.1 The Report has been prepared for the Comhairle's Audit and Scrutiny Committee. The original report advised of 10 recommendations made in the Cyber Attack Response report which was issued on 23 October 2024. The follow up review was undertaken in accordance with the operational annual internal audit plan for 2023/24.

Internal Audit Objective

1.2 Following up internal audit reports and assessing the level of compliance with recommendations made is an important part of the internal audit function.

1.3 In accordance with the remit detailed in the operational annual internal audit plan for 2023/24, our internal audit work was designed to obtain assurance that the original recommendations have been implemented. We obtained this assurance through internal audit testing and undertaking discussions with key personnel.

1.4 The main recommendations in the original report are all detailed in sections 1.5 and section 2 of this report.

Detailed Findings

1.5 The current status of progress against the original recommendations can be summarised as follows:

Key to Status

🟢 Fully implemented;

🟡 Partly implemented, although further work is required to meet the objective of the recommendation; or

🔴 Insufficient progress to date

Recommendations	Action to Date	Status
It is recommended to increase IT resiliency from cyber incidents to an appropriate level	Partly implemented	🟡
Implement the advice of the NCSC as well as following industry best practices in order to implement a series of additional security measures which are up to current global standards	Partly implemented	🟡
Install and train IT staff on the use of immutable backups, and ensure these are functional and up to date	Fully implemented	🟢
Undertake a review of systems which are not cloud based in order to ensure they still provide strong business continuity should we be subjected to a further attack. Cloud based systems already in place should also be reviewed to ensure they are adequate for the same business continuity requirements	Work still to be undertaken	🔴
As recommended by NCSC and the ICO, implement 24/7 endpoint monitoring as a permanent security solution	Partly implemented	🟡
Any future merger of the corporate and schools IT sections should ensure that they are maintained on separate networks to minimise any future cyber-attack impacts	Partly implemented	🟡
Where further improvements to IT security can be made, consider that these should be put forward to CMT and, if required, Members at the earliest opportunity should the costs involved be significant to the Comhairle	Work still to be undertaken	🔴
Investment in training and development should be planned as part of IT workforce plans from a staffing resiliency perspective	Partly implemented	🟡

Recommendations	Action to Date	Status
Ensure that training on cyber resiliency and awareness is mandatory for all staff and monitored closely to ensure the training itself remains relevant and that staff are undertaking said training	Partly implemented	●
Cyber Disaster Recovery Plans and Cyber Incident Response Plans as detailed in previous Audit Scotland recommendations, should be prepared and tested, primarily as a measure to enable appropriate responses to future attacks, attempted or actual	Partly implemented	●

Concluding Remarks

1.6 The report was only issued in full on the 23 October 2023 and recovery work is still ongoing. From our follow up testing so far, we note that out of the 10 recommendations made in the original report 1 has been fully implemented. We will continue to track progress and report this to the Audit & Scrutiny Committee.

1.7 For Comhairle Nan Eilean Siar Internal Audit Section

Internal Audit
Comhairle Nan Eilean Siar
Sandwick Road
Stornoway
Isle of Lewis
HS1 2BW

14 January 2025

SECTION 2 - DETAILED FINDINGS AND RECOMMENDATIONS

Action Recommended	Action By	Progress to Date	Action Outstanding
2.1			
It is recommended to increase IT resiliency from cyber incidents to an appropriate level	IT Manager	Key high value systems have been moved to the cloud and secured by the supplier. Further systems like website and forms also hosted off network and secured by the supplier. Network architecture made more secure. Ability to recover quicker implemented. Backups secured both on and off network. Monitoring and Logging 24/7 offsite implemented. Email security product implemented. The changes put in place spread the risk so any future incident should be isolated to a smaller part of the Comhairle's estate, the attack vector has also been significantly reduced due to the measures implemented.	Disaster recovery plan Cyber incident response plan Business continuity plan

Action Recommended	Action By	Progress to Date	Action Outstanding
2.2			
Implement the advice of the NCSC as well as following industry best practices to implement a series of additional security measures which are up to current global standards	IT Manager	Please see here for full details of the NCSC cyber security principals. [10 Steps to Cyber Security - NCSC.GOV.UK]	**Risk Management –** Detailed specific cyber security risks to be added to departmental risk register. **Asset Management –** Still to be reviewed to determine if there is

			anything that needs to be put in place.
		Engagement and Training – Information Security Training course updated. IT Manager engaging with Improvement Service regarding cyber security training to allow the usage of funding for section online training for whole department. IT regularly send out security updates to all staff.	IT Manager to review updates and authorise course to be deployed to all staff.
		Architecture and configuration – A redesign of our architecture was carried out and a multi-layer secure configuration put in place. Immutable backups on prem and in the cloud deployed and tested weekly. Email is protected via the Email Security blue print. Lateral movement significantly reduced. MXDR deployed. Management network significantly restricted.	Process to deal with Denial of Service attack
		Vulnerability Management – We run ad hoc Nessus scans across the network. Notifications from the Scottish Government monitored, 3rd party Cyber security sites regularly used to inform on latest threats.	Monitoring of large amounts of data leaving the network. Process to run Nessus regularly and issues addressed.
		Identity and access management – Geo locked MFA in place for all users including M365 admin users. Some systems do not have MFA capabilities built into them. Nobody is given access to data they don’t need access.	

		Data Security – Valuable cloud data is protected at rest and in transit via various methods: disk encryption, SSLVPN, IPSEC VPN. Only authorised users have access to council data. Email is protected via the Email Security blue print. Immutable backups on prem and in the cloud deployed and tested weekly. **Logging and Monitoring –** 24/7/365 Monitoring and logging has been put in place. **Incident management –** Cyber incident response plan currently being developed Supply Chain Security – Systems and Software are generally known as good, the Comhairle does not use unknown software on its estate, any cloud systems that are procured are asked for their responses to the NCSC 13 cloud principles and also their compliance with CAIQ framework is checked. Generally IT systems and products are bought through government frameworks which have additional controls in place for supply chain security.	Complete onboarding to the service and create playbooks for incidents detected. Testing and Exercise in a box when plans are complete.

Action Recommended	**Action By**	**Progress to Date**	**Action Outstanding**
2.3			
Install and train IT staff on the use of immutable backups, and ensure these are functional and up to date	IT Manager	Immutable backups deployed; responsible staff have been trained on the backup system.	None

Action Recommended	**Action By**	**Progress to Date**	**Action Outstanding**
2.4			
Undertake a review of systems which are not cloud based in order to ensure the still provide strong business continuity should we be subjected to a further attack. Cloud based systems already in place should also be reviewed to ensure they are adequate for the same business continuity requirements	IT Manager	No progress to date due to on premise still being rebuilt.	Whole Action

Action Recommended	**Action By**	**Progress to Date**	**Action Outstanding**
2.5			
As recommended by NCSC and the ICO, implement 24/7 endpoint monitoring as a permanent security solution	IT Manager	This is 95% complete the final element is to go through an onboarding exercise with the supplier to create customised playbooks for incidents detected and ensure configuration of the endpoint protection and alerting is correct.	Complete onboarding to the monitoring system

Action Recommended	Action By	Progress to Date	Action Outstanding
2.6			
Any future merger of the corporate and schools IT sections should ensure that they are maintained on separate networks to minimise any future cyber-attack impacts	Chief Officer Assets & Infrastructure/ Chief Officer Education & Children's Services	Document being prepared for consultation to commence January 2025.	

Action Recommended	Action By	Progress to Date	Action Outstanding
2.7			
Where further improvements to IT security can be made, consider that these should be put forward to CMT and, if required, Members at the earliest opportunity should the costs involved be significant to the Comhairle	IT Manager	No work has been carried out on this action point.	Whole action

Action Recommended	Action By	Progress to Date	Action Outstanding
2.8			
Investment in training and development should be planned as part of IT workforce plans from a staffing resiliency perspective.	IT Manager	IT Manager engaging with Improvement Service regarding cyber security training to allow the usage of funding to be used for a subscription to an online training platform so all the IT Section can benefit and upskill, if unsuccessful IT Manager will request budget to procure the platform internally.	Investment in training and development

Action Recommended	Action By	Progress to Date	Action Outstanding
2.9			
Ensure that training on cyber resiliency and awareness is mandatory for all staff and monitored closely to ensure the training itself remains relevant and that staff are undertaking said training.	Chief Officer HR & Performance	Internal Training and IT are developing an updated training course on cyber security. List of mandatory training courses now on LearnPro.	Communication on mandatory training will be circulated to all employees once cyber security training course ready for roll-out.

Action Recommended	Action By	Progress to Date	Action Outstanding
2.10			
Cyber Disaster Recovery Plans and Cyber Incident Response Plans as detailed in previous Audit Scotland recommendations, should be prepared and tested, primarily as a measure to enable appropriate responses to future attacks, attempted or actual	IT Manager	Cyber incident response plan, Disaster recovery plan and Business continuity plan are all currently in development.	Three plans highlighted to be ready for general use by 31st of March 2025.

APPENDIX

RESPECTIVE RESPONSIBILITIES OF MANAGEMENT AND INTERNAL AUDIT

Responsibility in Relation to Internal Controls

It is the responsibility of the Comhairle's management to maintain adequate and effective financial systems and to arrange for a system of internal controls. Our responsibility as internal auditors is to evaluate the financial systems and associated internal controls. In practice, we cannot examine every financial implication and accounting procedure within an activity, and we cannot substitute for management's responsibility to maintain adequate systems of internal controls over financial systems. We therefore may not identify all weaknesses that exist in this regard.

Responsibilities in Relation to Fraud and Corruption

The prime responsibility for the prevention and detection of fraud and irregularities rests with management. They also have a duty to take reasonable steps to limit the opportunity for corrupt practices. It is our responsibility to review the adequacy of these arrangements, but our work does not remove the possibility that fraud, corruption or irregularity may have occurred and remained undetected.

We nevertheless endeavour to plan our internal audit work so that we have reasonable expectation of detecting material fraud, but our examination should not be relied upon to disclose all such material frauds that may exist.