



To: Audit, Risk and Scrutiny Board

On: 19th January 2026

Report by: Head of Digital, Transformation and Customer Services

Heading: Audit Scotland Cyber Incident Findings: Comhairle nan Eilean Siar

1. Summary

- 1.1 A recent Audit Scotland¹ report following a cyber-attack on Comhairle nan Eilean Siar demonstrates that such incidents can cause prolonged disruption to critical services, including financial systems, leading to an inability to reliably manage the organisation's financial position and report this in the annual accounts.
- 1.2 Direct costs of recovery approached £1 million, with substantial additional indirect costs tied to service disruption, staff workload and delayed statutory duties.
- 1.3 The audit concluded that some previously agreed audit recommendations on business continuity arrangements and cyber resilience had not been fully implemented, suggesting stronger readiness and consistent follow through could mitigate future impacts.
- 1.4 The report emphasises that no public body is immune: design or structural differences do not guarantee safety and that all organisations must maintain robust cyber risk governance.

2. Recommendations

- 2.1 It is recommended that members of the Audit, Risk and Scrutiny Board note the contents of this report and note:
 - previous cyber security updates provided to the Board in relation to the Council's defence in depth and defence in breadth security architecture.
 - that further, more detailed, cyber security updates will be provided to the CMT in response to the findings.

¹ *Audit Scotland provides independent audit and assurance on how public bodies in Scotland manage and spend public money, helping to improve accountability, governance, and performance.*

- the criticality of business continuity arrangements, and the need for these to regularly reviewed by the relevant service and corporate owners.

3. Background

- 3.1. The report stems from the Audit Scotland audit into a 2023-24 cyber-attack on the Scottish local authority Comhairle nan Eilean Siar. It assessed the immediate and long-term impact on services, financial integrity, service delivery, auditability, and recovery operations.
- 3.2. Key findings included major disruption to financial systems, loss of data required for statutory accounting, delayed reporting and a resulting audit disclaimer due to insufficient audit evidence.
- 3.3. Financial costs were significant, not only immediate recovery expenses, but additional indirect costs due to resource diversion, increased manual workload, and reputational damage.
- 3.4. The audit noted that some earlier recommendations on business continuity, risk management and cyber resilience had not been fully actioned prior to the incident. This limited the authority's ability to respond effectively and recover promptly.
- 3.5. It further concluded that:
 - cyber risk must be managed as a strategic organisational risk, not just a technical ICT issue, with adequate governance, oversight, and resource allocation.
 - councils should prioritise business continuity planning and testing, stating that business continuity planning existed, but was not strong enough, not consistently applied, and not tested for a serious cyber incident materially affecting the response and recovery
 - recovery from a major cyber incident is long-term, not short-term. The report highlighted that systems and services were still being rebuilt almost two years later, demonstrating a sustained operational burden.

Implications of this report

1. Financial

The outcome of this report could result in additional costs to Renfrewshire Council dependent on any additional activities identified.

2. HR and Organisational Development

None directly arising from this report.

3. Community/Council Planning

None directly arising from this report.

4. Legal

None directly arising from this report.

5. Property/Assets

None directly arising from this report.

6. Information Technology

The outcome of this report could lead to additional ICT activities.

7. Equality and Human Rights

None directly arising from this report.

8. Health and Safety

None directly arising from this report.

9. Procurement

None directly arising from this report.

10. Risk

The outcome of this report could lead to additional risk activities.

11. Privacy Impact

None directly arising from this report.

12. Climate Risk -

None directly arising from this report.

13. Children's Rights – None directly arising from this report.

14. CoSLA Policy Position - None

List of Background Papers

Audit Scotland: Cyber-attack affecting operations and services: The 2023/24 audit of Comhairle nan Eilean Siar