Appendix 1

AUDIT REPORT 23'011

CYBER SECURITY

Executive Summary

The annual audit plan for 2022/23 provides for a review to be undertaken into the Council's arrangements surrounding its Cyber Security. Cyber Security concerns the protection of computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

The scope of this audit was to provide a review of systems, practices and an assessment of the controls in place to protect the Council from a cyber-attack. The audit also reviewed Information, Communication and Technology (ICT) security policies and procedures to ensure they are regularly reviewed and promote best practices. Cyber security controls are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside an organisation. A successful cyber-attack would immediately impact the delivery of services within the Council.

The Scottish Government in 2020 issued a Cyber Resilience Framework to all Local Authorities. The Cyber Resilience Framework was developed jointly between the Scottish Government and the National Cyber Resilience Advisory Board. The Framework includes a self-assessment tool to assist Local Authorities in improving their cyber resilience and compliance with a range of legislative, regulatory, policy and audit requirements regarding cyber security. The audit programme has been developed from this Cyber Resilience Framework and other good practice guidelines.

The audit was carried out in accordance with Public Sector Internal Audit Standards (PSIAS).

The review has highlighted the following areas for improvement:-

- The Scottish Government recommends that all Local Authorities should comply with the Scottish Government Cyber Resilience Framework. The Service has accepted the requirement to comply with the Framework by undertaking a self-assessment tool to highlight improvements needed to the Council's cyber resilience arrangements. It is appreciated that due to the pandemic, the ICT Service has been under additional pressure to meet changes in working practices across all Services. The audit found progress had been undertaken in completing the self-assessment tool; however, further action is needed to complete this review.

- It was found that no formalised incident response plan has been developed in the event of a successful cyber-attack. A cyber security incident response plan is a document that gives officers clear instructions on how to respond to

a serious security incident, such as a data breach, data leak, ransomware attack, or loss of sensitive information. Effective security controls would reduce the risk of a successful cyber-attack, however if the worse did occur, an incident response plan would ensure clear procedures are followed to limit the damage and disruption to Services.

- The Council has policies and guidelines detailing best practices that should be followed regarding information security and computer use. However, they have not been reviewed for several years. Policies and Guidelines should be reviewed and if required updated to include current best practices in information management, computer use and cyber security arrangements.

Recommendations

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
Key Control: Effective Cyber Security Controls to combat threats against networked systems and applications.						
5.01	The ICT Service should progress with completing the Scottish Government Cyber Resilience Framework self-assessment tool. Any improvement actions required to Council systems and procedures should be agreed with an action plan detailing recommendations for implementation.	High	Yes	In the latest response to the Scottish Government Cyber Assurance survey (Feb 22), the ICT Service reported that it currently aligns with the Progression Stage of 'Partial Target'. The intention is to progress to 'Target' by the end of the current financial year. Note there are dependencies on the	ICT Team Leader (Infrastructure & Information Security)	31 March 2023

Appendix 1

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
				implementation of 5.04 and 5.05		
5.02	ICT policies and guidelines should be reviewed and if required updated to include best practices in information management, computer use and cyber security practices.	Medium	Yes	The Corporate Information Security Policy is currently under review. A revised draft will be available by the end of September. The Computer Use Policy will be reviewed thereafter.	ICT Team Leader (Infrastructure & Information Security)	31 December 2022
5.03	The ICT Business Continuity Plan should be reviewed and if required updated to reflect current cyber resilience arrangements.	High	Yes	This was acknowledged in the response to the latest Scottish Government Cyber Assurance survey.	ICT Infrastructure Manager	31 December 2022

Appendix 1

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
5.04	Cyber security awareness training should be provided to officers of all levels within the Council.	Medium	Yes	A solution to provide phishing simulations and linked eLearning content, to raise cyber awareness has been procured. The work to implement this solution is in progress and discussions have taken place with regard to the baseline phishing campaign	ICT Team Leader (Infrastructure & Information Security)	31 March 2023
5.05	An Incident Response Plan should be developed and thereafter regularly tested through simulation exercises.	High	Yes	This was acknowledged in the response to the latest Scottish Government Cyber	Head of HR, ICT & OD / Infrastructure Manager	31 December 2022

Appendix 1

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
				Assurance survey. Work is also being progressed via CMT/SMT with regard to this, in light of the SEPA lessons learned.		
5.06	A review of existing insurance cover should be carried out to ensure the level of cover is appropriate and adequate in relation to the threat level from cyber-attack.	Medium	Yes	There is cover in the existing policy for reinstatement of data as well as cyber incidents. Further information is required on the obligations and requirements for cyber insurance in future renewals.	ICT Infrastructure Manager	30 September 2022