

Moray Council

Internal Audit Section

DEPARTMENT: Education, Communities & Organisational Development

SUBJECT: Cyber Security

REPORT REF: 23'011

Follow Up Audit Review

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)	Date of Completion	Status / Explanation	
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	31/03/23	Implemented - The self-assessment tool was completed in November 2022. An action plan to address identified areas of improvement has been developed.	

Moray Council

Internal Audit Section

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)	Date of Completion	Status / Explanation
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	31/12/22	Part Implemented – At the time of the follow-up review, both policies have been reviewed and remain at the draft stage. A revised implementation date has been agreed as 31/03/2024.
5.03	The ICT Business Continuity Plan should be reviewed and if required updated to reflect current cyber resilience arrangements.	High	Yes	31/12/22	Outstanding - This remains in progress with a revised implementation date agreed as 31/03/2024.
5.04	Cyber security awareness training should be provided to officers of all levels within the Council.	Medium	Yes	31/03/23	Implemented - An initial phishing exercise has been completed which will support a targeted approach to training. ICT has worked with the provider to agree topics to include within the training plan, now developed.
5.05	An Incident Response Plan should be developed and thereafter regularly tested through simulation exercises.	High	Yes	31/12/22	Part Implemented – An Incident Response Plan has been developed and discussed with the Corporate Management Team. Sessions

Moray Council

Internal Audit Section

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)	Date of Completion	Status / Explanation
					operated by Scottish Government and are due to be held in November 2023, thereafter the intention is to carry out simulation exercises locally. A revised implementation date has been agreed as 31/03/2024.
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	30/09/22	Implemented – ICT and Council Officers responsible for insurance have met with existing and wider insurers to discuss the level of cover available for cyber security. There are currently national issues relating to the level of cover available. This specific issue will continue to be discussed at annual review to ensure the Council can minimise the risks in this area.