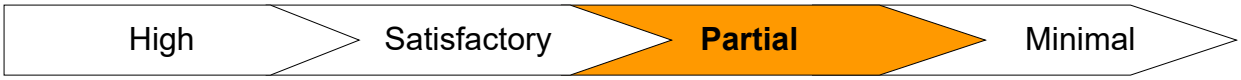
Appendix 2a: Audit Opinion and Themes

Assurance



Cyber Security – Awareness and Training

Objective

To assess the robustness and effectiveness of the arrangements to ensure all officers and Members have the necessary awareness to spot and avoid potential cyber security risks

Themes

A comprehensive and appropriate training programme is essential to ensure that all employees have an awareness of cyber security risks and issues, are vigilant to cyber-attacks and know what actions to take if the Council is subject to such an attack.

This audit focused on the training and awareness arrangements for officers and Members in reaction to potential cyber security risks.

In particular, we reviewed the monitoring of cyber training completion, and responsibilities of the training programme. We noted that there were inadequate processes and controls in place to ensure the training programme is completed, and that there is a lack of consequences for employees who do not meet their training responsibilities.

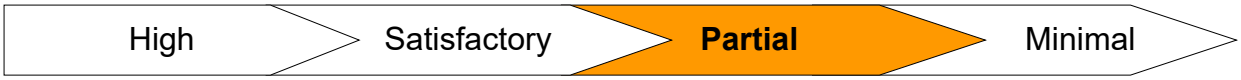
There is an opportunity to further strengthen the controls and processes as follows:

- Create and implement a policy dedicated to cyber security training or include the relevant content in another relevant policy. Having such a policy in place and available to all staff and Members will allow them to understand the expectations of them in their role by setting clear standards. This will ensure staff and Members understand that cyber security is a priority within the Council and help to foster a culture of security awareness. The policy would also demonstrate what they need to do to maintain an awareness of cyber security risks and issues and who to report or escalate to in the event of such an attack.

- Detailing clear roles and responsibilities for the key stakeholders involved in the cyber security training and awareness will help ensure that there is no confusion over individual roles, with the potential for duplication of effort, or important issues not being addressed. Each of those involved will be clear in what is required from them to ensure the training programme is delivered and driven effectively. It will also help enable improved teamwork and collaboration across these departments and eliminate any gaps in the process that currently exist.

Appendix 2a: Audit Opinion and Themes

Assurance



- Put in place measures to ensure that all staff and Members undertake and complete the mandatory modules within the set deadlines, and there are clear implications for employees who do not meet these targets. Ensuring that staff and Members are completing the necessary training will mean they are adequately prepared to identify or deal with cyber security threats leading to the potential for unauthorised access to Council systems, data breaches and financial losses. Additionally, no stakeholder has responsibility for ensuring that mandatory training requirements are met by Members.

- Ensure that those in the role of Digital Champion for their respective departments attend the annual cyber security workshops conducted by the IT Security team. As this role expects that they will then relay the training to their departments, it is imperative that these workshops are attended and the key messages disseminated in order for all email / IT users to receive the additional training, information and understanding.

- Follow up the completion of the automated Microsoft training that is assigned as a result of a failed phishing simulation to ensure that this has been undertaken. This data is currently available and monitored by IT Security, but is not actively chased for completion.

- Upgrade the current Learning Management System to allow managers within the Council to actively monitor the mandatory training completion rates of their teams. We noted that they are accountable to ensure that all staff and Members have completed their mandatory e-learning but have no way to effectively track this. We understand that these improvements have been proposed within the Council and are currently under consideration.

Number of actions agreed: 6