APPENDIX 4 – Executive Summaries of reports finalised

Cyber Security 2020/21

Overall conclusion on the system of internal control being maintained	**A**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
User Education and Awareness	**A**	**0**	**3**
Security Incident Management	**G**	**0**	**1**
Malware Protection	**A**	**0**	**4**
Vulnerability Assessments	**A**	**0**	**3**
Security Patching	**G**	**0**	**0**
Privileged Access	**A**	**0**	**3**
Remote Access	**G**	**0**	**1**
		0	**15**

Opinion: Amber	Final Report Issued: 20 July 2020	
Total: 15	Priority 1 = 0	Priority 2 = 15
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	15	

Cyber security remains a key area of business risk and shows no signs of abating given the seemingly endless reports on network security breaches, data breaches, ransomware, phishing and other types of cyber-attack. In this context, it is pleasing to see that Cherwell District Council have recently taken the step to recruit an IT and Cyber Security Officer, which will be a shared post with Oxfordshire County Council. This is a significant step forward that will help ensure there is clear ownership and focus on cyber security within the two organisations.

There are a number of corporate IT security policies available on the Intranet, however, they were found to lack details on some key areas of cyber security. The review also found that users do not have to acknowledge the existence of IT security policies and are not provided with mandatory training on cyber security to ensure they are aware of their responsibilities.

There is a documented Information Security Management Policy and a separate document on how to deal with a cyber incident. However, we found that it lacks details around the entire incident life-cycle and hence there is a risk that security breaches are not dealt with effectively to minimise the impact on the organisation.

Systems are in place to protect against malware threats but there are weaknesses in procedures and configurations that should be addressed to increase security levels.

There are regular security vulnerability scans and an annual IT Health Check (ITHC) in line with PSN requirements. There is an ongoing project that is addressing all reported vulnerabilities and weaknesses which is expected to complete by the end of June 2020. Whilst technical security penetration testing has been performed, a phishing test has not been commissioned to assess the level of risk exposure to phishing attacks.

There is a regular programme of applying security patches to client machines and infrastructure.

The number of IT users with domain wide administrator privileges was confirmed as being valid. However, the service accounts with this level of access should be reviewed, as well as users outside IT Services who have administrator access on specific servers. All default passwords are changed on infrastructure when it is initially built but we are recommending a scan to confirm that this is the case.

All remote access to the corporate network is secure and encrypted and changes are being made to Office 365 to enhance the levels of user authentication. We have identified a weakness in remote connections that should be addressed to reduce the risk of unauthorised access.

Definition of Internal Audit RAG opinions:

Grading:	**G**	**A**	**R**
Conclusion on:			
Overall conclusion on the system of internal control being maintained	There is a strong system of internal control in place and risks are being effectively managed. Some minor action may be required to improve controls.	There is generally a good system of internal control in place and the majority of risks are being effectively managed. However some action is required to improve controls.	The system of internal control is weak and risks are not being effectively managed. The system is open to the risk of significant error or abuse. Significant action is required to improve controls.