Outstanding Recommendations from Cyber Security Audit 2017/18

Audit Title	No of recommendation	Control	Priority	Responsible Officer(s)	Management Actions	Implementation Date	Commentary
Cyber Security 2017/18	10.8	Q.28 Are users prevented from running executable code or programs from any media to which they also have write access?	Medium	**Judith Doney**	**The Software Restriction Policy will be updated to prevent users from running executable code from any media to which they also have write access**	31 March 2019	Partially Completed - The ability to run executable code has been removed from the new Citrix installation, for everyone but technical staff. It is not possible to remove from the old Citrix installation due to lack of capacity.
Cyber Security 2017/18	10.10	Q.32 Are all application software security patches applied within 14 days of release?	Medium	**Judith Doney**	**The Council's capacity to re-write old software will be reviewed in the near future. Network segmentation, tight administrative controls and a thorough approach to logging and system data backup should be the next best control measures to adopt.**	31 March 2019	Not completed - Legacy software still in use and no action taken to address due to higher priority issues. However , legacy software will be addressed as part of our plans to rationalise the applications we use.
Cyber Security 2017/18	10.11	Q.33 Is all legacy or unsupported software isolated, disabled or removed from devices within the Scope?	Medium	**Judith Doney**	**See above action**	31 March 2019	Partially completed - On the new Citrix environment applications are delivered using layering. Going forward, redundant software will be removed. It is not possible to remove from the old Citrix installation due to lack of capacity.