Appendix 1: Overdue Audit Actions @ 15th March 2021

Reference	Audit Name and Action Number	Assignee	Detail	Evidence to be Provided	Current Due Target	Original Target Date	Status	Timing	Time lapse since original date
1137	Data Protection and Information Management 15.16	Oliver.morley	The Senior Information Risk Officer (SIRO) shall decide how long information and emails etc shall be kept within Anite, and the process for purging or archiving.	Decision taken and copy of instruction informing managers.	31/07/18	30/09/16	NotStarted	Late	4 years +
1496	Grounds Maintenance and Street Cleansing - 17.18 - 3	Neil.Sloper	In the period before the new cab system is implemented, the Street Cleansing and Grounds Maintenance manager will review a sample of maintenance sheets, this will be formally built into the new in cab solution in the future.	Reviewed beat sheets.	31/12/19	31/10/18	InProgress	Late	2 years+
1080	Social Media - 3a	gregg.sullivan	The Social Media Policy to include detail as to the types of posting that need to be formally reported as defamation or libellous to individuals or the Council. (in addition training to officers about the type of posting which fall into these categories should be provided).	The updated Social Media Policy that reflects the recommendations above.	31/03/20	31/01/19	NotStarted	Late	21 months
1133	Repairs & Maintenance of HDC property and equipment 17.18 - 4a	mark.houston	Once the plan of schedules repairs and maintenance has been compiled the service will agree key performance indicators to allow for performance to be monitored. (Appendix 1 in the report provides examples).	The agreed key performance indicators.	31/10/20	31/03/19	InProgress	Late	23 months
1170	Management of Health & Safety - 17.18 - 4	john.taylor	The following arrangements should be embedded into the Health and Safety policy: 1. Gas Safety 2. Infection Control 3. Respiratory Protective Equipment 4. Security Threats 5. Smoke Free Workplace 6. Transport Safety 7. Vibration	Updated Health & Safety policy.	30/09/19	31/03/19	NotStarted	Late	23 months
1339	Repairs & Maintenance of HDC property and equipment 17.18 - 3b	mark.houston	Once the asset management software has been purchased and populated with operational property details, the Facilities Management team will explore the use of the software with other managers who have responsibility for asset management.		31/03/20	31/03/19	InProgress	Late	23 months

1363	Repairs & Maintenance of HDC property and equipment 17.18 - 2	mark.houston	Once annual and cyclical plans have been compiled, a resourcing plan to evidence how these plans will be delivered - including financial budgets - will be prepared and approved by the Head of Operations and used to support the 2019/20 budget setting process.	The resourcing plan.	31/10/20	31/03/19	NotStarted	Late	23 months
1311	Repairs & Maintenance of HDC property and equipment 17.18 - 4b	mark.houston	If and when the Facilities Management team provide FM services for another team within the Council, service delivery expectations will be clearly defined, agreed and approved between the relevant Heads of Service.		31/10/20	31/03/20	InProgress	Late	11 months
1529	PCI DSS 18.19 / 3	Oliver.morley	A training needs assessment should be performed for all members of staff that have responsibility for PCI DSS compliance activities so as to determine their training needs.	Shared Service Management Board minutes	01/04/20	01/04/20	NotStarted	Late	11 months
1530	PCI DSS 18.19 / 4	Oliver.morley	Compliance should be monitored and actin taken when members of staff are found to have not completed the PCI DSS training or have not read the policy and procedures.	Shared Service Management Board minutes	01/04/20	01/04/20	NotStarted	Late	11 months
1531	PCI DSS 18.19 / 5	Oliver.morley	Actions need to be drawn together in a policy which sets out how the council will manage PCA DSS compliance activities and the policy should be reviewed on a regular basis. this should include but not be limited to: - Assignment of roles and responsibilities for ensuring that the Council is PCS DSS compliant - Procures for staff that are responsible for taking card payments - The Council's security strategy in relation to the storage, processing and transmission of credit card data - A set of instructions for detecting, responding to the storage, processing and transmission of credit card data.	Shared Service Management Board minutes	01/04/20	01/04/20	NotStarted	Late	11 months
1535	FMS Post-implementation 19.20 / 1	manjit.pope	Going forwards for joint projects key stakeholders (system users) from the Council should commit to the system specification phase and detail variances I business needs to ensure they are controlled and overseen.	System specifications	31/10/20	01/04/20	NotStarted	Late	11 months

1536	FMS Post-implementation 19.20 / 2	manjit.pope	Going forwards decision points such as UAT sign -off should be supported by contingency plans when partial roll out is approved. this should involve holding the vendor to account and /or providing additional resource to support processes.	Contingency plans.	31/10/20	01/04/20	NotStarted	Late	11 months
1537	FMS Post-implementation 19.20 / 3	manjit.pope	Going forwards all new contracts should stipulate an exit clause to ensure timely extraction and transformation of data from the legacy database to the new database.	Contractual agreements.	31/10/20	01/04/20	NotStarted	Late	11 months
1538	FMS Post-implementation 19.20 / 4	manjit.pope	Going forwards risk assessments as part of the initiation phase (project initiation document and project plan) should include an assessment of resource needs and corresponding resource risks.	Risk assessment	31/10/20	01/04/20	NotStarted	Late	11 months
1526	Protocol Policy Management System 18.19 / 3	madelaine.govier	Management will put a plan in place to seek staff awareness of IT policies by including a rolling awareness programme for extant policies within the protocol policy management system.	High level plan.	30/11/20	01/06/20	NotStarted	Late	9 months
1521	Hardware & Software Asset Management Control 19/20 / 8	Alex.Young	Procedures should be documented for the secure wiping of information when managing lost/stolen IT assets and prior to the disposal of IT assets.	Procedure to be developed for secure wipe/protection of data at rest for lost/stolen. supporting evidence - produce written documentation relating to Certificate revocation, bitlocker, intune remote wipe for phones, restrictions non re-introduction of devices on to the domain.	31/12/20	01/07/20	NotStarted	Late	8 months
1513	Access Management Control 19.20 / 5	Sagar.Roy	Head of IT & Digital 3C Shared Services should ensure requirements for setting up new user access to the network are set out in formal policy document and is uploaded onto the intranet and the PPMS. Line managers acknowledge the formal policy set out by 3CSS which ensures £CSS are notified of leavers in timely manner.	User access policy or requirements in an equivalent policy. Acknowledgement from line managers and employee owners.	31/08/20	31/08/20	InProgress	Late	6 months
1532	Network System Resilience & Availability 19.20 / 1	Alex.Young	Management should establish planned schedule for testing of data centre failover. Testing should be undertaken on at least an annual basis.	Data centre testing schedule.	31/10/20	31/10/20	NotStarted	Late	4 months
		Total: 19							