APPENDIX 1

High Priority					
Code	Title	Recommendation	Status	Due Date	Managed By
1819 Proc 14.01	Pentana Training & Procedures	a) Detailed procedures notes are developed for the use of the contract register on Pentana and made available to staff. b) Detailed training is provided to staff on the requirements of contract monitoring and management, how to use and update the contract register in Pentana to ensure staff are fully aware of their responsibilities and how to appropriately manage their contracts.	Overdue	30-Nov-23	Joanne Goodfellow
2021 PM 01	Asset Management Policy/Strategy	An Asset Management Policy and Strategy covering planned maintenance should be produced, approved and communicated with stakeholders. This should also include the frequency of the stock condition survey.	Overdue	30-Nov-22	Paul Weston
2122 PCI 01	PCI DSS Compliance	The PCI DSS Policy and Procedure should be reviewed and finalised. The policy should clearly define all key roles and responsibilities, including the corporate lead for PCI compliance.	Overdue	31-Dec-23	Joanne Goodfellow; Zoe Wolicki
2122 PCI 02	PCI DSS Compliance	The scope of the PCI environment should be explicitly defined, covering people, processes and technology. This should include a list of all service providers. Data flow maps may help define the PCI scope.	Overdue	31-Dec-23	Joanne Goodfellow; Zoe Wolicki
2122 PCI 03	PCI DSS Compliance	The relevant SAQ's should be identified and completed on an annual basis.	Overdue	31-Dec-23	Joanne Goodfellow; Zoe Wolicki

APPENDIX 1

2324 Bus Continu	01 Working group	A Business Continuity Working Group should be established to: . Oversee the review and testing of the Council's BCPs. . Report to senior management on business continuity activities. . Ensure that the BCPs align to the Council's corporate objectives. . Ensure stakeholders understand their roles and responsibilities for BCP. A terms of reference for the Working Group should be established, outlining the membership and role of the group.	Overdue	30-Sep-24	Paul Weston
2425 Cyber Sec	01 Security vulnerabilities report	A formal report on the status of all security vulnerabilities should be reported monthly to the Head of IT. A prioritised action plan should be agreed and risk mitigation put in place where possible. Vulnerabilities that cannot be immediately remediated or mitigated should be reported to CMT for acceptance.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
2425 Cyber Sec	02 IT Health assessment	All critical and high risk vulnerabilities on the RAP should be addressed as soon as possible. Risk mitigation and management processes should be established as per recommendation 1.	In Progress	31-Dec-24	Zoe Wolicki; Gareth Youlden