APPENDIX 2

Priority	Code	Title	Recommendation	Status	Due Date	Managed By
High	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
High	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
Low	2122 Creditors	01 Procedures	A review of guidance notes available on the intranet in relation to creditors should be reviewed and updated as required.	Overdue	31-Mar-23	Joanne Goodfellow; Zoe Wolicki
High	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
High	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.	Overdue	31-Dec-23	Joanne Goodfellow; Zoe Wolicki

APPENDIX 2

			Data flow maps may help define the PCI scope.			
High	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
Medium	2122 PCI 09	PCI DSS Compliance	Corporate level PCI compliant guidelines should be developed for all staff taking card payments.	Overdue	31-Dec-23	Joanne Goodfellow; Zoe Wolicki
Medium	2122 PCI 13	PCI DSS Compliance	Once the PCI scope is formally defined, discussions should be held with the acquiring bank to confirm what, if any, security scans are required.	Overdue	31-Dec-23	Joanne Goodfellow; Zoe Wolicki
Medium	2223 House Rents	02 Tenancy agreements	Signed tenancy agreements should be returned promptly.	Overdue	31-May-23	Hamid Khan; Tina Mustafa
Medium	2223 House Rents	03 Former tenant arrears	Consideration should be taken as to the suitability of tenants when renewing a tenancy, for instance their level of arrears. Whilst it is not current practice to transfer arrears to renewed tenancies, the former arrears should be subject to recovery action and payment plans should be set up.	Overdue	31-May-23	Hamid Khan; Tina Mustafa
Medium	2223 Landl/d H&S	01 Fire safety assessments	Confirmation should be sought that the actions have been addressed. Evidence of this should be retained.	Overdue	31-Mar-23	Paul Weston

APPENDIX 2

Medium	2223 Landl/d H&S	03 Electric inspections	The Electrical Inspection spreadsheet should be updated to include the commercial properties. The Council should continue to programme the electrical inspections in so that all properties are inspected.	Overdue	31-Dec-22	Paul Weston
Medium	2223 Landl/d H&S	04 Asbestos survey	All properties should have a completed asbestos survey, recorded correctly on the asbestos spreadsheet.	Overdue	31-Dec-22	Paul Weston
Medium	2223 Landl/d H&S	05 asbestos policy	The current processes should be reviewed to ensure compliance with the asbestos policy. For instance, clarity on whether asbestos management plan are site specific or strategic level. An asbestos annual report should be prepared for the Corporate Management Team.	Overdue	31-Oct-22	Paul Weston
Medium	2223 Landl/d H&S	06 Legionella remedial action	Remedial action to be taken on red issues and the Zetasafe dashboard should be updated with the current status.	Overdue	31-Dec-22	Paul Weston
Medium	2223 Landl/d H&S	07 Legionella risk assessments	There should be actions raised on Zetasafe/ Orchard to confirm the progress of the remedial work through to completion. Clarity should be obtained where the action is unclear.	Overdue	31-Dec-22	Paul Weston
Low	2223 Web Portals	17 accessibility statement	The MyHousing portal accessibility page should link to the web accessibility page on the corporate website.	Overdue	31-Dec-23	Zoe Wolicki; Gareth Youlden

APPENDIX 2

High	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
Medium	2324 Bus Continu	02 Training	All heads of service and BCP owners should be provided with training once their BCP has been refreshed. This should then be provided on an agreed basis thereafter. Where staff have specific roles or responsibilities in the BCP, tailored training should be provided to ensure they fully understand their responsibilities. Training compliance rates should be monitored by the Assistant Director of Assets.	In Progress	31-Dec-24	Paul Weston
Medium	2324 Bus Continu	03 BCP's	Each service area lead should review and revise the BCPs to ensure that they are completed using the latest template. The plans should specify a clear BIA which set out the critical functions for the service, including RTOs and RPOs. The plans should be subject to review on at least an annual basis.	Overdue	30-Sep-24	Paul Weston

APPENDIX 2

Low	2324 Comm safety	03 CSP plan	The council should develop clear aims and objective for the CSP plan which should be set out at the start of the plan. These should be linked with the identified priorities and give direction for the workplan to be based on.	In Progress	31-Mar-25	Joanne Sands
Medium	2324 Corp Policy	01 Policy log	A policy log should be developed containing all organisational policies which includes the following information: Policy Owner Last review date Review Frequency Next review date Whether it should be uploaded on to Astute The responsibility of who has oversight of the log should be determined to ensure that policy owners are regularly reviewing and updating their policies when required. This could be for the whole Council or specific service areas.	Overdue	30-Jun-24	Zoe Wolicki
Medium	2324 Corp Policy	02 Policy ownership	Heads of Services should be reminded of their responsibility to update policies within their service area. Policies should be reviewed in line with what is stated within the coversheet. Each policy should include a standardised coversheet which outlines the responsible individual and approval history.	Overdue	30-Jun-24	Zoe Wolicki

APPENDIX 2

Low	2324 Creditors	02 Receipts	In line with Recommendation 1A and 1B, the requirements to retain receipts and the ramifications of not doing so should be clearly outlined in the credit card policy.	Overdue	30-Apr-24	Emma Dyer; Joanne Goodfellow
Low	2324 Insurance	01 Policies and procedures	Information including policies and procedure notes to be reviewed to ensure relevance and accuracy.	Overdue	30-Sep-24	Emma Dyer; Joanne Goodfellow; Omotayo Lawal
Low	2324 Insurance	04 Safe controls	It should be considered that a reminder email be sent to Managers. The email should include the Financial Guidance requirements, in relation to keys and also inform of the insurance cover of the safe.	Overdue	29-Feb-24	Emma Dyer; Joanne Goodfellow; Omotayo Lawal
Medium	2324 Insurance	02 Renewal procedures	Procedures should be developed to cover the renewal process. This should include a checklist of tasks that can be used to monitor progress and return of information requested. The checklist should include responsible officers and timescales.	Overdue	30-Sep-24	Emma Dyer; Joanne Goodfellow; Omotayo Lawal
Medium	2324 Insurance	03 Invitation to quote	The invitation to quote form should comply with the Financial Guidance.	Overdue	31-Mar-24	Emma Dyer; Joanne Goodfellow; Omotayo Lawal
Low	2324 Remote	IT Remote Working 11	The information on MS Teams should include a link to the training videos and associated material available on the Microsoft website.	Overdue	30-Nov-23	Pardeep Kataria

APPENDIX 2

Low	2324 Risk Mgt	03 Training	A risk management training programme should be provided to all staff to ensure there is clear guidance on their roles and responsibilities, and how departmental risks feed into the corporate risk areas. This could be in an e-learning module so staff can access the content at any time or through in-house training. We recognise that the Council would need to firstly consider its resources to deliver this additional training.	In Progress	31-Mar-25	Emma Dyer; Joanne Goodfellow

APPENDIX 2

Medium	2324 Risk Mgt	01 Review and monitoring	1. The Senior Management Team should continue to review the control measures for the risks identified on the Corporate Risk Register quarterly. This should include scrutiny of the detail provided on the control measures to identify what the 'actual' controls are. Controls which the Council may wish to consider include for Risk 7 are: . Cyber security and data protection training, including simulated exercises to test awareness eg phishing exercises. . Technical controls that are in place on the Council's network such as multi-factor authentication and restriction of web content. . Testing of the Council's business continuity and disaster recovery procedures. 2. Risk management training should be provided to the Audit and Governance Committee to ensure it has the appropriate skills to effectively undertake its role for overseeing and monitoring risks.	Overdue	31-May-24	Emma Dyer; Joanne Goodfellow

APPENDIX 2

Medium	2324 Risk Mgt	02 Local Risk Register	1. In accordance with Finding 4, further training should be provided to staff, outlining the roles and responsibilities for risk management and providing support on how to effectively document controls. 2. Each Head of Service should present the local risk register to the Assistant Director responsible for the area quarterly to oversee the implementation of the control measures.	In Progress	31-Mar-25	Emma Dyer; Joanne Goodfellow
Medium	2324 Safeguardin	02 New starter training	Training should be provided within 3 months of starting employment.	Overdue	31-Jan-24	Jackie Noble; Joanne Sands
Medium	2324 Safeguardin	03 Refresher training	Refresher training should be completed every 3 years.	Overdue	31-Mar-24	Jackie Noble; Joanne Sands
Medium	2324 Safeguardin	04 training consistency	Officers of the same role should receive consistent safeguarding training. Training should be monitored and chased to confirm completion.	Overdue	31-Mar-24	Jackie Noble; Joanne Sands
Medium	2324 Safeguardin	06 Sheltered scheme	Confirmation should be recorded that the DBS check has been seen for service provider, for instance the DBS certificate number.	Overdue	31-Jan-24	Joanne Sands

APPENDIX 2

Low	2324 T & D	05 Policy	• Following the implementation of the new Training and Development Policy, it should be reviewed and updated every three years to ensure it reflects the Council's current arrangements. • The new draft Training and Development Policy should be updated to include the following before it is implemented: • References to how training modules can be completed on Astute or via alternative methods (see Finding 4) • Consequences for non-compliance with the policy requirement, ie disciplinary actions for non-completion of mandatory training.	Overdue	30-Jun-24	Jackie Noble
Medium	2324 T & D	02 PDR completion	The HR team should continue to monitor completion of PDRs at the end of the PDR window. A reminder email should be issued to line managers and staff that have not completed their PDR with ongoing non-compliance reported to CMT listing those PDRs that remain outstanding two weeks after the window.	Overdue	31-Aug-24	Jackie Noble

APPENDIX 2

Medium	2324 T & D	03 PDR analysis	• Heads of Services and Assistant Directors should meet annually after the PDR window to identify priorities in their service's needs and advise the Head of Human Resources and Organisational Development on the training allocation suggestions. To identify high performers, the Council should consider whether to utilise a rating system into its PDR process. This could be used to direct the Heads of Service and Assistant Directors on staff that would benefit from further training.	Overdue	31-Aug-24	Jackie Noble
Medium	2324 T & D	04 Training delivery	The Council should explore alternative approaches to delivering mandatory training modules to staff in manual roles. For example, these could be completed by face-to-face group sessions or 'Toolbox Talks'. However, if these options are pursued then attendance records should be maintained to ensure the HR and Organisational Development Team can track completion of mandatory training.	Overdue	30-Jun-24	Jackie Noble

APPENDIX 2

Medium	2324 Taxi Lic	01 Checks	A. The details of the exceptions identified in our testing will be shared with the lead officer and these should be investigated further to ensure they are rectified at the earliest opportunity. B. Going forwards, the Council should ensure all steps and documentation requirements set out in the Policy are completed prior to issuing licences and that ongoing checks are completed to ensure these remain up-to-date. The findings from this report should be shared with all relevant staff, highlighting the common issues identified and reminding staff of the correct Policy. Failures to comply should be escalated and actions taken as appropriate. C. The Council should investigate whether it would be feasible to update the M3 System to add functions with automatic alerts on expired or missing documentation, to ensure sufficient controls are in place to identify out-of-date information. The results of these enquiries should be formally documented, including any alternative options and costings.	Overdue	30-Apr-24	Wendy Smith

APPENDIX 2

High	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
High	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
Low	2425 Cyber Sec	10 CMT info	CMT should be briefed every six-months on cyber security and related matters.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	11 Phishing training	Users who fail the phishing test should be required to complete additional cyber training.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	12 Microsoft defender	As planned, Microsoft Defender should be installed on all mobile devices.	In Progress	31-Dec-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	13 Sophos	The Sophos threat protection policies for clients and servers should be reviewed.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	14 Scan of clients	The Sophos threat protection policies for clients and servers should be reviewed.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	15 Daily job list	The check of Sophos Central should be added to the daily checks job list.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	16 Application control policy	The application control policy on Sophos should be reviewed.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden

APPENDIX 2

Low	2425 Cyber Sec	17 Default administrator account	The name of the default administrator account should be changed and the account disabled if it is not used.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Low	2425 Cyber Sec	18 Vulnerability Management Policy	The Vulnerability Management Policy should be reviewed and updated.	Overdue	30-Sep-24	Zoe Wolicki; Gareth Youlden
Medium	2425 Cyber Sec	03 Cyber risk	A cyber risk should be added to the IT risk register and all existing risks reviewed. Cyber should also be added to the corporate risk register for senior management oversight.	In Progress	31-Dec-24	Zoe Wolicki; Gareth Youlden
Medium	2425 Cyber Sec	04 Training	Cyber security training should be refreshed annually.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Medium	2425 Cyber Sec	06 Administrator accounts	Administrator accounts should not be used for web browsing or accessing emails. Separate non-administration accounts should be used for these activities.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Medium	2425 Cyber Sec	07 LAPS	The issue with LAPS should be resolved and it should be used for all clients and servers.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Medium	2425 Cyber Sec	08 Workstation Admin Group	Users in the Workstation Admin Group should be reviewed.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden
Medium	2425 Cyber Sec	09 Microsoft Intune reporting	Microsoft Intune reporting on patch status should be reviewed and all computers confirmed to be patched up-to-date. A formal check should be performed monthly.	In Progress	31-Oct-24	Zoe Wolicki; Gareth Youlden

APPENDIX 2

Low	2425 Debtors	01 Corporate Credit Policy	The Corporate Credit Policy should be reviewed to ensure it is reflects the current owner and actual procedures.	In Progress	30-Nov-24	Faron Blencoe; Michael Buckland
Medium	2425 Debtors	03 invoice promptness	Invoices should be raised promptly. Supporting documentation should be retained to confirm the charge, or if needed, if a dispute should arise. Officers should be reminded to put their contact details on the invoice.	In Progress	31-Dec-24	Faron Blencoe
Low	2425 Food Safety	01 Procedures	Work should continue to review the procedures to ensure a complete and current set is available for staff.	In Progress	31-Dec-24	Wendy Smith
Low	2425 Food Safety	03 Filing paperwork	Officers should ensure that all paperwork is correctly filed under the correct premise.	In Progress	31-Dec-24	Wendy Smith
Medium	2425 Food Safety	02 registrations	Following receipt of submitted forms, new businesses should be promptly registered and follow the inspection pattern. Where there are reasons for a delay, for instance, the business has not started operating, this should be recorded on the notes.	In Progress	31-Dec-24	Wendy Smith
Medium	2425 Food Safety	04 Inspections	Inspections should be completed at the frequency the risk category dictates.	In Progress	31-Dec-24	Wendy Smith

This page is intentionally left blank