Appendix 3

Summary of Recommendations and Management Responses from Internal Audit Reports issued Quarter 3, 2019/20

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
Corporate Governance – 5 December 2019				
4.2.12	Completed gifts and hospitality forms should be covered by the corporate document retention policy.	Low	Democratic Services Manager & Deputy Monitoring Officer	Details of how this will operate to be discussed with the Information Governance Manager with the aim of putting process in place by end of the financial year. TID: 31 March 2020
4.3.12	Minutes should be taken for all meetings of the Risk Management Group, with nominated 'deputies' taking minutes when the Insurance & Risk Officer is unable to attend.	Low	Audit & Risk Manager	Agreed. TID: Immediate

[1] Risk Ratings are defined as follows:

High:	Issue of significant importance requiring urgent attention.
Medium:	Issue of moderate importance requiring prompt attention.
Low:	Issue of minor importance requiring attention.

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
4.3.14	Consideration should be given to the remit of the group and whether there is a need for a specific group or if these discussions could be covered by SMT when they consider the Significant Business Risk Register.	Low	Audit & Risk Manager	We have considered this and feel that common themes are emerging, albeit not necessarily reflected in the minutes. There is tremendous benefit in hearing about other services' risks as there are always lessons to be learned corporately and we feel that this is the right forum to provide that opportunity. These issues do need to be captured better and, perhaps more importantly, communicated "outwards" more effectively so that, indeed, lessons can be learned across the organisation. This will be considered at the next meeting. TID: Not applicable.
Planning Policy – December 2019				
No recommendations arising from review on this occasion.				
Sundry Debtors – 28 November 2019				
4.2.3	Except in exceptional cases, which should be agreed by the Head of Finance, invoices should be issued before services have been provided. Where invoices are not issued in advance, the circumstances should be recorded and kept under review by the relevant Head of Service and Head of Finance. Where there is no pre-agreed reason for the delay, the relevant Head of Service should provide authorisation explaining the reason for the delay when submitting the documentation for the raising of the invoice.	Low	Head of Finance	A meeting is going to be held to decide how the recommendations will be actioned. TID: End of December 2019

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
Treasury Management – 9 October 2019				
4.2.3	The Treasury Management Practice statements should be revised to reflect the proper status of Internal Audit in the control environment and risk-based determination of audit frequencies.	Low	Principal Accountant (Capital and Treasury)	The Treasury Management Practices will be reviewed for the 2020/21 Treasury Management Strategy. TID: February 2020
Infrastructure Security and Resilience – 29 October 2019				
4.5.3	Firewall appliances should be upgraded to CISCO's recommended Code version.	Medium	ICT Services Manager	Agreed. Some of the Council's firewalls are currently being replaced. Once this is complete, all remaining Firewalls will be updated and maintained to Cisco's latest recommended code version. TID: April 2020
4.6.4	The Cisco 'Password Policy' security settings should be reviewed to enforce password history (12) and password minimum length (8).	Low	ICT Services Manager	Agreed. The Council operates several Firewalls and the changes need to be implemented cautiously to avoid lockouts. TID: January 2020

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
4.8.4	The Cisco IPS system should be actively configured to block all malicious network traffic.	Medium	ICT Services Manager	Agreed. IPS was originally configured to run in monitoring mode to obtain sufficient data to identify network false positives. Discussions were already being undertaken at the time of the audit to schedule an appropriate time for IPS to become active. TID: February 2020
Information Systems Policies – 25 October 2019				
4.3.3	The 'Information Security Incident Reporting' policy should be reviewed and updated.	Medium	Information Governance Manager	The policy is already under review with target completion date (for adoption) of December 2019. TID: 23 December 2019
4.4.1	Ongoing work to update data retention, data handling and classification policies should be completed and updated policies should be made available to staff.	Medium	Information Governance Manager	The polices are already under review with target completion date (for adoption) of December 2019. TID: 23 December 2019
4.4.2	Data retention schedules should be brought up to date and a regular review process should be introduced.	Medium	Information Governance Manager	This is not the responsibility of the IG Manager but the relevant service areas. However, the IG Manager is in the process of working with all Teams (within departments to remind them about these and to bring them up to date). TID: Not applicable

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
4.7.3	All remaining policies should be reviewed and updated.	Medium	Information Governance Manager	The polices are already under review with target completion date (for adoption) of December 2019. TID: 23 December 2019
4.9.3	An exercise to review the accuracy and completeness of the Council's record of processing activities should be undertaken on a regular basis to ensure the record is up to date. Management should also consider audits of individual departments to verify the accuracy of data in the record.	Medium	Information Governance Manager	The IG Manager has been meeting with teams within Service Areas as in parallel to the retention schedules. However, part of this action should be for all Heads of Services (as Data Asset Owners) to ensure these records are correct. Also, both this and retention schedule should be an area that Audit test as part of their routine audits of each service area to validate the processes. Not applicable.
Cloud Applications – 25 October 2019				
4.2.3	The 'Privacy Impact Assessment Toolkit' document should be reviewed and updated.	Medium	Information Governance Manager (Shafim Kauser)	The review of the toolkit is currently under way, along with the rest of the Information Governance Framework, and this will be completed by 23 December 2019. TID: 23 December 2019
4.2.4	The 'Software Policy' should be updated to reference the 'Privacy Impact Assessment Toolkit' process.	Low	ICT Services Manager (Ty Walter)	Accepted: The Software Policy has been updated to reflect the PIA Toolkit requirements (03 Oct 2019), and this version is now available via the ICT Policy pages on the Intranet. TID: Not applicable.

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
4.3.4	Management should liaise with the supplier to increase Get Scheduled password complexity requirements.	Medium	Get Scheduled System Owner (Jessica Craddock)	I had spoken with the system owner and system developer (Tom Douglas & Wojciech Dragan) to implement the complexity requirements. Passwords for each user now requires a minimum of 8 characters including 1 special character, 1 uppercase and 1 number. This was actioned by all users w/c 23.09.19. TID: Not applicable – recommendation actioned.
4.3.5	Management should investigate options around implementing two factor authentication to the ArtifaxEvent application.	Medium	ArtifaxEvent System Owner (Laura Wyatt)	We have tested the two-factor authentication provided by the ArtifaxEvent system. As the system heavily relies on mobile phone signage and the phone reception at the Royal Spa Centre being so poor we are unable to switch this on. It would potentially mean locking our users out of the system when they required necessary information for events. TID: Not applicable recommendation not accepted.
4.4.5	The privacy impact assessment process should be completed retrospectively for the ArtifaxEvent system.	Medium	ArtifaxEvent System Owner (Laura Wyatt)	To be arranged and completed. TID: 31 December 2019.
Catering Concessions – 19 December 2019				
No recommendations arising from review on this occasion.				

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
Health and Safety Compliance of Council Buildings – 4 November 2019				
4.2.9	A review should be undertaken of the properties with 'active' EICR attributes on Active H to ensure that this accurately reflects the properties for which EICR tests are required.	Low	Data Coordinator (DC) and M&E & Energy Officer (MEEO)	Agreed. DC and MEEO to identify all stock requiring cyclical EICR's and update attributes in ActiveH accordingly. Further, a semi-automated programme of works can be generated as demonstrated in other areas. TID: 31 March 2020
4.2.12	A schedule of PAT testing should be set for each relevant Council property.	Low	DC and MEEO	Agreed. DC and MEEO to identify all stock requiring cyclical PATesting and update attributes in ActiveH accordingly. Further, a semi-automated programme of works can be generated as demonstrated in other areas. TID: 31 March 2020
4.2.14	Inventories of electrical equipment that require PAT testing should be maintained for each relevant Council property.	Low	Asset Compliance & Delivery Group (AC&DG), MEEO & Dodds	Agreed, the AC&DG need to agree that building managers maintain an inventory of equipment requiring PATesting. Dodds should be able to support with information of equipment currently tested. TID: 31 March 2020
4.3.3	The variation to the original contract should be confirmed with D&K.	Low	Compliance Team Leader (CTL)	A copy of the variation documentation has now been obtained. TID: Completed.

Report Reference	Recommendation	Risk Rating[1]	Responsible Officer	Management Response and Target Implementation Date (TID)
4.5.12	Inventories of fire-fighting equipment should be kept up to date to ensure that contractors are aware of what needs to be tested.	Low	AC&DG, MEEO & Baydale	Agreed, the AC&DG need to agree that building managers maintain an inventory of equipment pertaining to fire-fighting equipment. Baydale should be able to supply information of currently installed equipment. TID: 31 March 2020
4.7.5	Training on the need for Permits to Work should be provided to relevant staff, including individual building managers as appropriate.	Medium	CTL, Building Manager & H&S Coordinator (BM&HSC) and AC&DG	Agreed. CTL and BM&HSC to liaise on suitable training and audience. TID: 31 January 2020
Food Safety – 26 November 2019				
No recommendations arising from review on this occasion.				
Homelessness and Housing Advice – 5 December 2019				
4.3.11	Refresher training on the setting up of rent accounts on Active H should be given to relevant staff.	Low	Senior Housing Advice Officer	The team have a number of new and inexperienced staff. We will arrange refresher training for the relevant staff on setting up rent accounts. TID: 31 December 2019
4.5.4	Staff should be reminded of the need to ensure documents are attached appropriately to the system.	Low	Senior Housing Advice Officer	We will arrange refresher training for the relevant staff on document management. TID: 31 December 2019
Open Spaces – 14 October 2019				
No recommendations arising from review on this occasion.				