

Cotswold District Council

Report of Internal Audit Activity

January 2021

Contents

The contacts at SWAP in connection with this report are:

David Hill

Chief Executive

Tel: 01935 848540

david.hill@swapaudit.co.uk

Lucy Cater

Assistant Director

Tel: 01285 623340

lucy.cater@swapaudit.co.uk

- Appendices:

Appendix A – Internal Audit Definitions	Page 5 – 6
Appendix B – Audit Plan Progress	Page 7 - 11
Appendix C – Summary of Audit Findings	Page 12 – 16
Appendix D – High Priority Findings and Agreed Actions	Page 17 – 22
Appendix E – Summary of Agreed Actions	Page 23

At the conclusion of audit assignment work each review is awarded a “Control Assurance Definition”;

- **No**
- **Limited**
- **Reasonable**
- **Substantial**

•

Audit Framework Definitions

Control Assurance Definitions

No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Non-Opinion – In addition to our opinion based work we will provide consultancy services. The “advice” offered by Internal Audit in its consultancy role may include risk analysis and evaluation, developing potential solutions to problems and providing controls assurance. Consultancy services from Internal Audit offer management the added benefit of being delivered by people with a good understanding of the overall risk, control and governance concerns and priorities of the organisation.

Recommendations are prioritised from 1 to 3 on how important they are to the service/area audited. These are not necessarily how important they are to the organisation at a corporate level.

Each audit covers key risks. For each audit a risk assessment is undertaken whereby with management risks for the review are assessed at the Corporate inherent level (the risk of exposure with no controls in place) and then once the audit is complete the Auditors assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

Audit Framework Definitions

Categorisation of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors; however, the definitions imply the importance.

	Categorisation of Recommendations
Priority 1	Findings that are fundamental to the integrity of the service's business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management
Priority 3	Finding that requires attention.

Definitions of Risk

Risk	Reporting Implications
High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.
Medium	Issues which should be addressed by management in their areas of responsibility.
Low	Issues of a minor nature or best practice where some improvement can be made.

Audit Plan Progress

APPENDIX B

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
						2019/20 Audits in Draft / In Progress at Annual Opinion			
Key Financial Control	Accounts Receivable		Final Report	Reasonable	4		1	3	Reported in November
Follow-Up	S106 Agreements and Funds		Draft Report						
Follow-Up	Procurement		Final Report	N/A	-				Reported in November
Follow-Up	Procurement and Contract Management		Final Report	N/A	-				Reported in November
Operational	Asset Management and Commercial / Investment Property		Draft Position Statement						
Advisory	Use of Volunteers		Final Report	N/A	-				Reported in October
Advisory	Grants		Final Report	N/A	-				
ICT	Business Continuity		Draft Report						
ICT	Incident Management		Final Report	Reasonable	4		2	2	See Appendix C

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
2020/21 Audit Plan									
Operational	Business Grant Funding		Complete	N/A	-				Support to the Council in respect of Data Input
Advisory	Leisure Funding		Complete	N/A	-				Support to the Council in respect of the Leisure Funding request by the Service Provider
Advisory	CFU Policies		Complete	N/A	-				Reviewing policies held by CFU and advising of changes to legislation
Operational	Continuous Assurance Reports		On-Going						Accounts Payable, Accounts Receivable, Payroll
Support	Business Grant Funding (Part 2)			N/A	-				Head of IA seconded to Council to support processing of Mandatory and Discretionary Business Grants during from November onwards
Key Financial Control	Revenues and Benefits								
	• Council Tax and National Non-Domestic Rates		Draft Report						
	• Housing and Council Tax Benefits		Draft Report						
Key Financial Control	Core Financials								
	• Accounts Payable		In Progress						
	• Accounts Receivable								

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
	• Main Accounting		In Progress						
	• Payroll		In Progress						
	• Treasury Management and Bank Reconciliation		Final Report	Substantial	1			1	See Appendix C
Key Financial Control	Systems Administration		In Progress						
Key Financial Control	Human Resources								
Key Financial Control	Other Support Service provided by Publica • Health and Safety (Of Staff)		Position Statement	N/A					See Appendix C
ICT	Cyber Security		Final Report	N/A	5			5	See Appendix C
ICT	Use of Anti-Malware Software		ToE Drafted						
ICT	Automatic Back-Up of System Data								
Governance	Risk Management								
Governance	Performance Management								
Governance	Governance of Programmes and Projects								
Operational	Post Payment Assurance – Small Business Grants								
Operational	Authority's Response to Covid-19								

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
Operational	Publica Transformation Benefits Realisation								
Operational	The Delivery of Services by Publica								
Operational	Inclusivity and Diversity								
Operational	Publica Support Costs Recharge Process & Internal Control Process for Contract Variations (NEW)		ToE Agreed						
Advisory	Implementation of the New Revenues and Benefits System		In Progress						Support to the Project Team
Follow-Up	Follow-Ups of Recommendations made in Substantial and Reasonable Audits		On Going						
Follow-Up	Follow-Up of Control Weaknesses identified by the Counter Fraud Unit								
Follow-Up	Procurement								Further Follow-Up required
Follow-Up	Procurement and Contract Management								Further Follow-Up required
Grant Certification	Disabled Facilities Grants		Complete	N/A					
Grant Certification	Income Compensation Scheme (NEW)								
Other Audit Involvement	Working with the Counter Fraud Unit		On Going						


Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
Other Audit Involvement	Management of the IA Function and Client Support		On Going						
Other Audit Involvement	Contingency – Provision for New Work based on emerging risks								






The following information provides a brief summary of each audit review finalised since the last Committee update

ICT Incident Management – Final Report – December 2020

Audit Objective

The objective of the audit is to ensure that technical solutions are managed and deployed to protect data and systems from malicious attack.

Assurance Opinion		Number of Actions		Risks Reviewed	Assessment
	<p>There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.</p>	Priority 1	0	<p>Operation of the network or information systems is disrupted. Information and data are intercepted and disclosed or stolen.</p>	<p>Medium</p>
		Priority 2	2		
		Priority 3	2		
		Total	4		

Key Findings	Audit Scope
 <p>As part of the Information Security framework of policies, the Incident Management Policy is out of date and requires review, update, and approval. Update of the policies has been impacted by the Covid-19 pandemic, and the need for a review is recognised by the ICT Audit & Compliance Manager.</p>	<p>The audit scope was a review and assessment of the policies, plans and processes in place and used together with technology used to detect, prevent, and respond to security incidents or events.</p> <p>The review also covered the following areas;</p> <ul style="list-style-type: none"> Threat detection and protection Vulnerability assessment and remediation <p>The review was undertaken by interviewing key personnel including the Cyber Security Engineer and the ICT Audit and Compliance Manager, together with the review of documentation and evidence provided.</p>
 <p>There is a lack of detailed standard operating procedural documentation. Incident management investigation is currently based on a high-level process flow-chart denoted in the Incident Management policy; however, this lacks detailed information on how to conduct an incident investigation.</p>	
 <p>At the initial stages of the audit there was a limited Incident Response plan. It is best practice to develop risk-based scenarios within response plans and regularly test them to prepare for an incident. A detailed plan noting scenarios and action plans is being developed and good progress has been made.</p>	
 <p>Weekly vulnerability scans are performed, and prioritised vulnerabilities where remedial action is to be taken are actioned using the helpdesk ticketing system. A similar process could be used to track all vulnerabilities detected in the weekly scans as is used for the annual penetration test findings.</p>	
 <p>Appropriate technology is in place and used to enable the Cyber Security Engineer and wider ICT team to detect, mitigate and respond to security incidents. The Cyber Security Engineer practices continual education and development to keep abreast of current technology, threats, and risks.</p>	

Next Steps

It is widely recognised that for any organisation, a significant security incident or breach is a matter of 'when', not 'if'. Organisations are increasingly reliant on IT services, therefore, it is critical that an organisation is prepared, as much as possible, for a significant incident that will disrupt ICT service provision.

Actions have been agreed with management, with a detailed action plan attached as Appendix 1, to improve incident management preparedness. All actions are due to be implemented by April 2021 or are ongoing exercises. A summary of the key findings from our review will be presented to the Audit Committees and Publica Board.

Unrestricted

Unrestricted

Health & Safety of Staff – Position Statement – December 2020

Audit Conclusion

A Health & Safety of Staff review was included in the 2020/21 Annual Internal Audit Plan. The focus of the audit was planned to be on site visits and use of Personal Protection Equipment (PPE) in relation to hazardous substances. Initial meetings were held with the Health and Safety Business Partner (H&S BP) for Publica to discuss the scope of the audit.

The initial focus of the audit was set prior to COVID-19, where it would have been possible to carry out testing with officers and service areas in person, allowing us to review and provide assurance on practical control arrangements in place which would be most appropriate based on the audit focus. Following initial meetings with the H&S BP, we have agreed that due to the remote working arrangements currently in place, it would provide limited value in carrying out the audit at this time.

Based on discussions with the H&S BP, we have no immediate concerns in this area. We have also agreed with the H&S BP that internal audit will accompany them in a sample of their planned future Health and Safety audits relating to the Control of Substances Hazardous to Health (COSHH) and PPE to provide oversight.

We have issued this Position Statement which provides information on where the service is at this current time.

- A Health and Safety Audit schedule has been commenced and covers all service areas to be audited between October 2020 and April 2024.
- The Publica Property Services Health and Safety audit was most recently completed (October 2020) and action plan was issued to the service area to address any findings made.
- A local Health and Safety Committee was re-established in September 2020, covering Publica, Cotswold District Council, West Oxfordshire District Council and Forest of Dean District Council.
- The Group Manager – Business Support Services provided the Annual Health and Safety Update to the Publica Board on the 4th of September 2020 and will also provide quarterly updates going forward.

Cyber Security Follow Up Report – October 2020

Audit Objective

To follow up on the 2018/19 recommendations and consider areas for further review in 2020/21.

Executive Summary and conclusion

During 2018/19 a Cyber Security audit was undertaken by SWAP's ICT audit team for Publica and the Partner Councils. The audit was based on a framework of 20 Key Cyber Security controls which covered 32 areas ranging from policy to technology. The audit was a 'high level' audit and testing was undertaken between April and July 2019 to determine whether:

- The control was fully compliant
- Management needed to take action
- Further audit testing (in an area) was to be planned

Due to the ever-changing nature of ICT, we included a subsequent review in the revised 2020/21 Internal Audit Plan. Supported by Publica's ICT Audit and Compliance Manager, we have followed-up the recommendations made in the 2018/19 audit and planned the audits which were identified as warranting a more in-depth audit.

Fully Compliant Areas

The original audit confirmed that the following areas were compliant, therefore no recommendations were made, and no further audit was required:

Control	Area
Inventory of Software Assets (Including Data Assets)	Data Asset Inventory
Control of Accounts with Administrative Privileges	Management of Default passwords for high privileged accounts
Active Monitoring and Analysis of Audit Logs	Audit Logging and Retention Policy
E-mail and Web Browser protections	Use of Network Based URL Filters / Blocking of Uncategorised Websites
Control of Network Ports, Protocols and Services	Documentation and authorisation routines for ports, Protocols and Services
Secure Configuration of Network Devices	Build standards and management process for network devices
Boundary Defences are documented and understood	Management of connections across trusted network boundaries
Programme of Penetration testing	Conducting and following up on penetration testing

Recommendations Made

Thirteen recommendations were made in the 2018/19 audit. This review has found that:

- Seven recommendations have been actioned
- One recommendation is an on-going piece of work and will remain live
- The progress on four recommendations has been affected by Covid-19. The implementation date for these recommendations was June / September 2020. We have agreed with the ICT Audit and Compliance Manager to defer the implementation dates to allow for the recommendation to be actioned. We will follow these up when the target date has been met.
- A recommendation that was made in respect of Asset Lifecycle Management will be planned to be included in the 2021/22 Audit Plan within the Technology Asset Inventory Audit.

Further Audit

An outcome of the audit undertaken in 2018/19 was to enable us to plan the ICT audits going forward, there are areas that we have reviewed at a high level but warrant further audit testing to gain full assurance over the management of risk. IA and the ICT Audit and Compliance Manager have assessed these areas based on the level of risk to Publica and the partner Councils.

Full details of our audit testing/ working papers are available upon request. Our audit assurance framework and definitions can be found here (www.swapaudit.co.uk/aboutus)

Treasury Management and Bank Reconciliation – Final Report – January 2021

Audit Objective

To ensure that the key controls within Treasury Management and Bank Reconciliations are operating effectively.

Assurance Opinion	Number of Actions	
	Priority	Number
	Priority 1	0
	Priority 2	0
	Priority 3	1
	Total	1



A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Risks Reviewed	Assessment
1. Inadequate treasury management arrangements in place, resulting in financial loss.	Low
2. If bank reconciliations are not regularly carried out, there is a risk of inaccurate financial reporting, loss of income and fraud.	Low
3. If previous recommendations made are not implemented, the organisation may be open to unnecessary risk exposure	Low

Key Findings

	One Priority 3 recommendation is still outstanding from the 2018/19 Treasury Management and Bank Reconciliations audit. The Business Partner Accountant has committed to completing the agreed action by the end of January 2021.
	A new cashflow monitoring spreadsheet has been implemented at WODC which is updated monthly by the Senior Technical Accountant and provides an easy to view summary for the Chief Finance Officer. This is also planned to be replicated for the other Councils.
	Bank reconciliations sampled were found to be accurate and signed off by an appropriately senior and independent officer.

Audit Scope

A high-level review will be completed in the following areas:

- Follow up on last year's recommendations
- Treasury Management reporting process
- Cashflow forecasting

Discussions were held with the Publica Business Partner Accountant and the Senior Accounting Technician. Evidence to support discussions was requested where appropriate.

Bank statements and the bank reconciliations from October 2020 were reviewed for all Councils and Publica.

Next Steps

One action has been agreed with management, attached as Appendix 1. All actions are due to be implemented by the 31st of January 2021. We will follow up to assess progress towards the agreed priority 3 action in due course. A summary of the key findings from our review will be presented to the Audit Committees and Publica Board.

Unrestricted

Full details of our audit testing are available upon request. Our audit assurance framework and definitions can be found here (www.swapaudit.co.uk/audit-framework-and-definitions)

High Priority Findings and Agreed Actions

APPENDIX D

Audit Name	Priority	Agreed Actions	Agreed Action	Due Date	Update January 2021
ICT Incident Management 44560	2	As part of the Information Security framework of policies, the Incident Management Policy is out of date and requires review, update, and approval. Update of the policies has been impacted by the Covid-19 pandemic, and the need for a review is recognised by the ICT Audit & Compliance Manager.	ICT Audit and Compliance Manager will review and update all ICT Security Policies following the completion of the Cyber Security audit report. The aim to have drafted policies by April 2021 for circulation to all network users.	Apr 2021	
ICT Incident Management 44562	2	There is a lack of detailed standard operating procedural documentation. Incident management investigation is currently based on a high-level process flow-chart denoted in the Incident Management policy; however, this lacks detailed information on how to conduct an incident investigation.	We have now commenced with documenting our cyber incident and investigation managements procedures	On Going	
Payroll 43699	2	We recommend that all new starters are subject to a BPSS (or similar) check regardless of the role to which they are being recruited. This will ensure that consistent checks of right to work, employment history and basic criminal record checks are carried out on all employees.	A piece of work has been carried out to re-write the pre-employment check process. The HR and Recruitment Teams are also working towards the implementation of an Application Tracking System (ATS), subject to approval at Publica and the Councils, which would help to mitigate the risks identified. The ATS would not allow for progression in the recruitment and onboarding process without specific criteria being fulfilled first (e.g. obtaining references, ID checks etc).	Sep 2020	Will be followed-up during the annual audit

High Priority Findings and Agreed Actions

APPENDIX D

Audit Name	Priority	Agreed Actions	Agreed Action	Due Date	Update January 2021
Health and Safety – Fire Risk Assessments 43147	2	We recommend that officers should ensure all remedial actions identified in fire risk assessments are completed using a risk-based approach.	These remedial action requirements are in progress and will be completed in accordance with the noted time scale.	Sep 2020	Will be followed-up within the Health and Safety Audit
Procurement and Contract Management 41127	2	We recommend that assurance is sought from Publica that contracts held and managed on behalf of the Council are monitored and managed effectively.	Publica colleagues have been requested to respond to the recommendations made in the report issued. Assurance has been requested that contract management and monitoring is undertaken.	Sep 2020	Implementation date changed to 31st December 2020 to reflect amended target implementation date of majority of Procurement/Procurement & Contract Management recommendations to be actioned by Publica Procurement.
Accounts Receivable 43752	2	Duplicate subscriptions should be reviewed, and appropriate corrections made. Any duplicate payments should be returned to the debtor.	All subscriptions will be corrected where applicable. Will discuss with team to ensure that prior to setting up new subscriptions a search for existing subscriptions is performed. If any queries arise the AR officer will refer to the service area for clarification. Responsible Officer – AR Team Leader	Aug 2020	Will be followed-up during the annual audit
Section 106 Agreements and Funds	2	To ensure the Council can be held to account in managing the delivery of S106 obligations, the progress of S106 Agreements should be regularly reported at an appropriate Committee and on the Council's website.	Once the Government has produced the data specification and collection tools, these will be used to produce reports for Members and published on the Council's website. There is currently no known date for the publication of these tools, therefore a prolonged timescale has been proposed to implement this action.	Mar 2020	Officers responsible for agreeing, recording and monitoring S106 at FoDDC, CDC & WODC met 23/09/19 to discuss strategies for aligning best practice across the partner councils. Implementation of this recommendation is progressing and will continue to be monitored by IA This needs to be followed up, it is likely that Covid-19 has delayed the implementation of this recommendation

High Priority Findings and Agreed Actions

APPENDIX D

Audit Name	Priority	Agreed Actions	Agreed Action	Due Date	Update January 2021
Systems Admin 41204	2	We recommend a principal Identity and Access Management process detailing requirements for 'Joiners, Movers and Leavers' is developed and documented and that complies with the requirements set out in the Information Security and Access Control Policy. The overarching process should apply to and embrace all systems that may not be included within the standard ICT team scope and should be available for all employees to view and follow. System administrators should then document or update local processes and procedures that should be in alignment with the overarching policy and process requirements. and documented on a quarterly basis as per the requirements of the Risk Management Policy	Our team ICT Administrators are now updating and documenting our Access Management system process for joiners, Movers and Leavers. A change control process will be introduced that will document significant changes to the ICT infrastructure which will also align to our ICT User Policies and guidance.	Mar 2020	<p>Flowcharts have been produced for the starters / leavers / variation processes.</p> <p>The ICT Audit and Compliance Manager will refresh the ICT Policies following the completion of the Cyber Security audit report. He is aiming to have drafted policies by March 2020 for circulation / consultation at CGG and JMT.</p> <p>Further follow-up has been included in the 2020/21 audit plan</p> <p>Revised implementation date to 31/12/20 due to Covid-19</p>

High Priority Findings and Agreed Actions

APPENDIX D

Audit Name	Priority	Agreed Actions	Agreed Action	Due Date	Update January 2021
Apprenticeship Scheme 42609	2	We recommend that a reconciliation process is implemented for Apprenticeship Levy payments.	<p>Reconciliation is now carried out monthly between the Finance spreadsheet, the General Ledger and the online apprenticeship levy portal. Support will be requested from Finance to ensure reconciliation is being done correctly in the initial stages.</p> <p>The internal apprentice recruitment form has also been amended to ensure that the recruiting manager consults with the Finance Department to ensure there is appropriate levy funding available in the online account before the post goes for approval at the Resource Managers Group.</p>	Implemented & ongoing (to be followed up Feb 2020)	Recommendation followed up but no response was received from the service. Due to the lapse in time the recommendation has been closed.
Procurement 41030	2	To ensure there is an audit trail to support all contract payments, the introduction of "No PO, no payment" policy should be considered to assist with the efficient monitoring of contract spend.	This will be considered	Dec 2019	We were advised that no decision has been made yet regarding the implementation of a 'no PO, no pay' policy across the Publica Councils. Proposals will need to be submitted by Publica for consideration by Cabinet and the Leadership Team at each Council. This recommendation will require further follow-up in 2020/21.
Procurement 41002	2	<p>All Officers should be informed during Procurement Process training of the following to ensure when applicable;</p> <ul style="list-style-type: none"> • Procurement are consulted on all contracts over £5,000 so all approved contracts are entered onto the Contract Register, and waiver details can be accurately recorded when appropriate 	Agreed	Dec 2019	Training has not yet been fully delivered which includes officers' responsibilities and instruction that Procurement are required to publish all spend over £5000 and therefore must have sight of all spend. Procurement approval is required for all acquisitions over £10,000 on Agresso Business World (ABW) which will help to ensure Procurement are aware of spend over £5000 and will also allow them to identify where a waiver is used so this can be appropriately recorded. This recommendation will require further follow-up in 2020/21.

High Priority Findings and Agreed Actions

APPENDIX D

Audit Name	Priority	Agreed Actions	Agreed Action	Due Date	Update January 2021
Procurement 41323	2	To ensure all transactions are raised and approved appropriately and in line with the current organisational structure, all requisitioning and approval permissions should be reviewed in BWO.	Following the recent organisation changes, the approvals permissions will be reviewed to ensure they are aligned with new roles and implemented accordingly on the ABW system.	Dec 2019	<p>We were advised:</p> <ul style="list-style-type: none"> •A review of ABW requisitioner and approver roles is currently in progress. •Together with the finance team, the ABW support team aim to review all clients over the coming months. •A review of roles at both Ubico and CBC are complete. Work on CDC approvers is still underway. This recommendation will require further follow-up in 2020/21.
Procurement 41181	2	A copy of the approved contract must be held on In-Tend for all contracts over £5,000, as well as the quotes used during the tendering process, to demonstrate best value and ensure there is a complete central record.	Agreed, subject to a review of the contract value requirements.	Dec 2019	<p>The Senior Procurement Business Partner demonstrated the Contracts Module on In-Tend during fieldwork. We were advised that all new contracts since the implementation of the Contracts Module (October 2019) have been input into In-Tend. These contracts are being managed by the Procurement Team via this system in terms of monitoring of contract expiry dates.</p> <p>We were able to confirm all relevant documentation (including a copy of the approved contract) was stored for the sampled CBC contract.</p> <p>We were advised by the Senior Procurement Business Partner that it is intended that contracts that were already in place at the time that the Contracts Module was implemented will be loaded into the system in the same way as new contracts, but the speed at which this can be done is dependent on available resources to carry out the work.</p> <p>To assist them in managing existing and future contracts, the Procurement Team have implemented a future Work Plan for all authorities.</p> <p>Revised implementation date to 31/12/20 due to Covid-19</p>

High Priority Findings and Agreed Actions

APPENDIX D

Audit Name	Priority	Agreed Actions	Agreed Action	Due Date	Update January 2021
Procurement 41029	2	Budget Holders should regularly undertake monitoring of expected contract spend to actual contract spend as part of contract monitoring, to ensure contracts are managed in accordance with strategy, and inform Procurement of any changes to contract values to ensure the values recorded on the Contract Register are correct.	Agreed	Dec 2019	No evidence has been provided of actions carried out by responsible officers to support implementation of this recommendation at the time of follow-up. As part of the 2020/21 Audit Plan, an audit of the Management and Monitoring Contracts will be carried out. The scope of this audit will include budget monitoring arrangements in relation to contract spend and will therefore inform the follow-up of this recommendation. Revised implementation date to 31/12/20 due to Covid-19

Summary of all Agreed Actions from April 2019 and Progress against them

CDC ONLY	Priority			
	1	2	3	Total
TOTAL in Audit Period (From 4/19)	0	1	4	5
Open and current	0	0	0	0
Open and Outstanding/Overdue Subject to follow up	0	0	1	1
Open with date extended	0	1	3	4
Closed	0	0	0	0

PUB ONLY	Priority			
	1	2	3	Total
TOTAL in Audit Period (From 4/19)	0	8	9	17
Open and current	0	2	6	8
Open and Outstanding/Overdue Subject to follow up	0	2	0	2
Open with date extended	0	3	2	5
Closed	0	1	1	2

