

APPENDIX 1

Internal Audit reports finalised since the February 2017 Audit Committee meeting

Audit Title:	Stores and Equipment Management – Follow Up						
Date of Report:	January 2017			Materiality/Impact:		High	
Number of ‘High Priority’ Recommendations:	1	Current Audit Opinion:	3	Previous Audit Opinion:	3	Overall Evaluation (Risk):	Of concern
<p><u>Key Recommendations</u></p> <p>Since the previous audit, there has been clear engagement of responsible officers to undertake improvements and implement the recommendations from the original audit. As a result, fourteen of the eighteen recommendations made in the previous audit have either been implemented or partially implemented.</p> <p>However, one key, high risk recommendation has not yet been fully implemented, which relates to the introduction of a new tool and plant equipment register. An old and unsupported version of DATAstox is still currently in use as the equipment management system and therefore the inherent risk to the safety of staff (and the exposure to the Council that this presents) means it is not appropriate to change the level of audit opinion at this stage. It should be clear that the responsibility for this recommendation is the Fleet and Workshops Team (rather than Stores), who are progressing with the process of implementing a new software system, it is understood that the system has received IT approval and will now be procured (after which further time will be required to ensure records going forward are up to date and reliable).</p> <p>Regarding Stores specifically, the follow up has found that there are no outstanding high risk areas and any remaining, lower priority recommendations not yet fully implemented are considered to be in hand and covered within the current Stores Action Plan.</p>							

Audit Title:	NNDR						
Date of Report:	6 th February 2017			Materiality/Impact:		High	
Number of 'High Priority' Recommendations:	0	Current Audit Opinion:	2	Previous Audit Opinion:	1	Overall Evaluation (Risk):	Moderate
<u>Key Recommendations</u> There are no key recommendations as a result of the review.							

APPENDIX 1

Audit Title:	Cheque Refunds Investigation					Date of Report:		11/10/16		
Date of Report:		February 2017			Materiality/Impact:			Medium		
Number of ‘High Priority’ Recommendations:		N/A	Current Audit Opinion:		N/A	Previous Audit Opinion:		N/A	Overall Evaluation (Risk):	N/A
A review of cheque refunds and payments was conducted following instances of fraud by a member of staff were identified during an investigation conducted in response to a whistleblowing allegation. No recommendations were made during the review.										

Audit Title:	Safeguarding (CSE)						
Date of Report:	February 2017			Materiality/Impact:		Medium	
Number of 'High Priority' Recommendations:	6	Current Audit Opinion:	3	Previous Audit Opinion:	n/a	Overall Evaluation (Risk):	Moderate
<u>Key Recommendations</u>							
The key recommendations made as a result of the review are:							
<ul style="list-style-type: none"> • The Council's Strategy to Prevent Child Sexual Exploitation should be reviewed, and updated as appropriate, to reflect current knowledge and understanding of the prevalence of CSE locally and nationally, along with the Council's objectives and intended outcomes. • The Council should continue to use its data to inform practice and direct activities. To supplement this, discussions should be held with Wiltshire Police to establish whether they could expand the contents of the Partnership Profile in order to provide more detailed underlying data to support the themes identified from analysis of information held. • The Delivery Plan should be updated to ensure that it clearly reflects the objectives of the revised CSE Strategy • In accordance with the CSE Strategy and Terms of Reference for the CSE Working Group, Lead Officers should provide timely, accurate updates of their actions. • When the CSE Delivery Plan is revised, agreed actions should be documented in detail in order to ensure that progress and outcomes are clear and understood to allow for accurate status reporting and monitoring. • The Council's Corporate Management Team should monitor the effectiveness of the CSE Strategy and Delivery Plan. 							

APPENDIX 1

Audit Title:	IT Training							
Date of Report:	March 2017				Materiality/Impact:		High	
Number of 'High Priority' Recommendations:	4	Current Audit Opinion:	3	Previous Audit Opinion:	N/A	Overall Evaluation (Risk):	Of Concern	

Key Recommendations

The key recommendations made as a result of the review are:

- The review of the terms of reference for the Council's Information Governance Group should be completed and the Board re-established. It should meet at appropriate points in the year to ensure adequate arrangements for information governance are in place. This should include overseeing the implementation of recommendations made in this report and management of associated risks.
- A report should be created to enable monitoring of whether all staff have completed and passed the mandatory e-learning modules as and when required. This report should be sent to the relevant officers to enable monitoring of compliance rates to take place and for issues to be escalated as appropriate e.g. to Corporate Management Team or the Information Governance Group. Senior management and Heads of Service should review reports regularly to ensure compliance with mandatory training requirements.
Failure to comply with the mandatory training requirements should ultimately result in the user being prevented from accessing the Council's network, confidential or sensitive information.
- Mandatory training requirements for temporary staff, consultants, agency staff and members should be agreed and communicated. Reports on completion of mandatory training requirements should be provided for all those with access to the Council's data e.g. consultants, temporary staff, agency staff etc. and provided to the relevant officers as required.
- Reports on all information security incidents should be compiled and reported to an appropriate forum (which includes the SIRO and the Monitoring Officer), who should provide oversight to ensure that an appropriate corporate response is taken to information risks identified. Reporting on data protection breaches should continue to be reported to the Data Protection Officer and then to an appropriate forum as mentioned above.

APPENDIX 1

Audit Title:	Debtors 2016/17						
Date of Report:	March 2017			Materiality/Impact:		High	
Number of 'High Priority' Recommendations:	0	Current Audit Opinion:	2	Previous Audit Opinion:	1	Overall Evaluation (Risk):	Moderate
<u>Key Recommendations</u> There are no key recommendations as a result of the review.							

Audit Title:	Investigations						
Date of Report:	February / March 2017			Materiality/Impact:		N/A	
Number of 'High Priority' Recommendations:	N/A	Current Audit Opinion:	N/A	Previous Audit Opinion:	N/A	Overall Evaluation (Risk):	N/A
<u>A number of investigations have also been completed:</u> <ul style="list-style-type: none"> • Inv. 16/17-11 • WB 16/17-3: general issues 							

The following audit reports are currently out in draft:

- IT Governance and Policies
- Street Works
- Forward Swindon
- Emergency Duty Service
- Main Accounting
- Fleet Management
- Oracle system control
- Compliance with Contract Standing Orders
- Children's Health
- Commercial Assets
- Housing Rents
- Registrars
- ID Badges