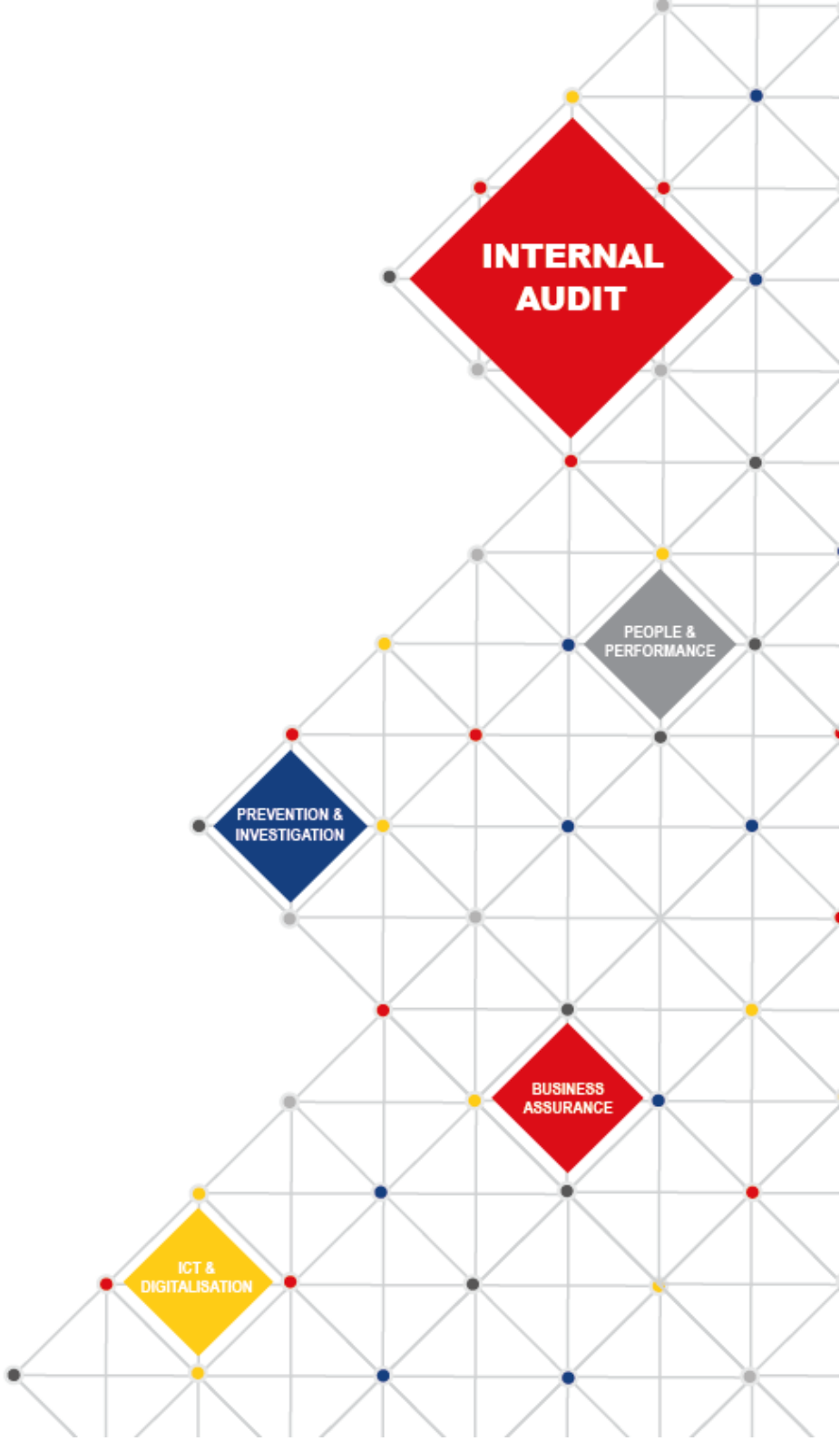
tiaa

Chiltern District Council

Internal Audit Progress Report

Audit and Standards Committee 16 July 2018

FINAL



2018/19

INTRODUCTION

1. This summary report provides the Audit Committee with an update on the progress of our work at Chiltern District Council as at 26 June 2018.

PROGRESS AGAINST THE 2018/19 ANNUAL PLAN

2. Our progress against the Annual Plan for 2018-19 is set out in Appendix A. The results of these reviews are summarised at Appendix B.

EMERGING GOVERNANCE, RISK AND INTERNAL CONTROL RELATED ISSUES

3. We have not identified any emerging risks which could impact on the overall effectiveness of the governance, risk and internal control framework of the organisation.

AUDITS COMPLETED SINCE THE LAST REPORT TO COMMITTEE

4. The table below sets out details of audits finalised since the previous meeting of the Audit and Standards Committee. Final reports with priority 1 and 2 recommendations are shown at Appendix B.

		Key Dates			Number of Recommendations			
Review	Evaluation	Draft issued	Responses Received	Final issued	1	2	3	OEM*
Car Parking	Substantial	6/03/18	16/03/28	20/03/18	-	-	-	2
Cash and Bank	Substantial	16/02/18	20/03/18	26/03/18	-	-	-	-
Cemeteries	Substantial	8/02/18	1/03/18	21/03/18	-	-	1	-
Data Protection	Reasonable	20/04/18	15/06/18	18/06/18	-	4	1	2
Ground Maintenance	Reasonable	21/02/18	27/02/18	28/02/18	-	1	2	-
Housing Benefits	Substantial **	20/12/17**	20/03/18**	27/03/18	-	-	-	-
ICT – Network Controls	Reasonable	6/12/17	15/12/18	29/01/18	-	2	3	-
Treasury Management	Substantial	21/02/18	28/02/18	5/03/18	-	-	1	1

*Operational Effectiveness Matters (these are good practice suggestions that have arisen during the audit)
**The delay in receiving management's response to the draft report was because officers did not appreciate a response was required on a substantial assurance audit with no recommendations.

CHANGES TO THE ANNUAL PLAN 2018/19

5. The following changes have been made to the audit plan for 2018/19

Review	In strategic plan for 2018/19	Change made	Rationale for the change
HR Absence Management	Omitted in error	An addition to the plan	This audit was carried forward from 2017/18 and initially missed from the 2018/19 plan
ICT Members ICT Support	Yes	Delete	
ICT Cyber Security	Yes	Delete	Covered by the PSN review audit not required
ICT User Access to Business Systems	Yes	Delete	Covered by the PSN review audit not required

FRAUDS/IRREGULARITIES

6. We have not been advised of any frauds or irregularities in the period since the last summary report was issued.

LIAISON

7. We liaise with EY and provide reports and working paper files, as required.

We have regular client meetings with the Audit, Fraud and Error Reduction Manager and Head of finance

PROGRESS ACTIONING PRIORITY 1 RECOMMENDATIONS

8. We have not made any Priority 1 recommendations (i.e. fundamental control issue on which action should be taken immediately) since the previous Progress Report

RISK MANAGEMENT

9. The Audit Director with TIAA and the Councils Audit, Fraud & Error Reduction Manager meet on a regular basis to discuss and action Risk Management matters for both Councils.

The current Risk Procedures/Guidance for Risk Management is being reviewed and progress is being made to display appropriate information on Risk Management throughout both Councils. This will include posters on all notice boards at the main civic offices for South Bucks and Chiltern Councils, as well as data on the Councils intranet.

Appropriate training has been developed and has been delivered on “Risk Management in a Changing Environment” for all middle managers. Further training has been scheduled for June and July 2018.

RESPONSIBILITY/DISCLAIMER

9. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. The matters raised in this report not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Progress against the Annual Plan for 2018/19

System	Planned Quarter	Days	Current Status	Comments
Governance	3	8		
Risk Management	3	8		
Procurement	2	8		
Counter Fraud	1	8		
Data Protection	2	8		
Business Continuity	2	7		
Purchase Cards	2	8		
Expenses	1	8	In progress	
Project Management	2	8		
Main Accounting	3 or 4	7		
Payroll	3 or 4	15		
Accounts Receivable (Debtors)	3 or 4	8		
Accounts Payable (Creditors)	3 or 4	8		
Benefits	3 or 4	13		
Council Tax Support	3 or 4	13		
Council Tax and NDR	3 or 4	25		
Cash and Bank	3 or 4	7		
Budgetary Control	3 or 4	7		
ICT - Annual Network Audit	3 or 4	6		

System	Planned Quarter	Days	Current Status	Comments
ICT - GDPR	**2**	**6**		
ICT - Customer Experience	**2**	**6**		
ICT – Members ICT Support		0(6)		Cancelled
ICT – Cyber Security		0(6)		Cancelled
ICT – User Access to Business Systems		0(8)		Cancelled
Temporary Accommodation follow up	2	8		
Housing Section 106	2	8		
Disabilities Facilities Grant	1	5	Draft report issued 20 June 2018	
Safeguarding	1	6	In progress	
Chiltern Pools	2	8		
Health & Safety Contractor Arrangements	2	8		
New Chiltern Car Park	4	8		
Property & Asset Management	2	8	In progress	
Planning Development & Enforcement	2	11		
Building Control	1	8	In progress	
HR - Absence Management	4	8		Additional audit carried forward from 2017/18
Crematorium				
Annual Internal Audit	1	6	Draft report issued 22 June 2018	
Additional Audit	1	6		

KEY:

	=	To be commenced
	=	Site work commenced
	=	Draft report issued
	=	Final report issued

Appendix B

Audits Finalised since last Audit Committee

Title of review: **Data Protection** Date issued: **18 June 2018**

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Directed	The Joint Data Protection and Confidentiality Policy is due to be reviewed annually, however the current policy is dated February 2016. There are separate ICT Security Policies in place for both Councils; for CDC the majority of the policy sections are dated 2011, including an out of date Data Protection Policy, and the SBDC ICT Security Policy is dated August 2014. Other policies which require review include the Joint Protective Marking Scheme (dated May 2014), the Data Breach Policy (dated November 2009, and South Bucks only), the Joint Guidance on Data Protection and Freedom of Information (dated August 2015), and the Joint Records Retention and Disposal Policy (dated June 2016 and due to be reviewed annually).	Policies and procedures relating to Data Protection and Information Governance be reviewed at the earliest opportunity, with a timetable put in place for completion.	2	*Reviews of these documents had been delayed awaiting publication of final versions of GDPR & DP 2018 Act. The work was further impacted by the illness of the Corporate Information Manager and their absence from the office.* *Other members of Business Support have picked up the work to review and publish updated versions of required documents.*	*30/06/2018*	*HoBS*

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Operational	As part of the departmental sample testing, discussions with officers highlighted some concerns that the last training received was October 2017, and that further training should be taking place during 2018 in the build up to GDPR implementation at the end of May. The GDPR implementation plan also states that Management Team/Heads of Service/middle managers must undertake Data Protection/GDPR corporate training. This action had a scheduled completion date of 27 February 2018, however discussions with Heads of Service indicated that this training had yet not been provided at the time of writing (April 2018).	Further GDPR training sessions be provided at the earliest opportunity to ensure that Information Asset Owners and Information Asset Administrators across the Council are fully aware of the actions required prior to GDPR implementation.	2	*This work has also been impacted by the ill health of the Corporate Information Manager and their absence from the office.* *External trainers have been booked to deliver specialist training for Information Asset Administrators and this will take place by the end of July.* *Online training provided by the LGA for members, and Learning Pool, the Councils' online training resource for all staff who will be required to undertake awareness training on the new legislative changes.*	*31/07/2018*	*HoBS*

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Operational	The documenting of processing activities is a new requirement under the GDPR. Information that must be documented includes: the purposes of the processing; a description of the categories of individuals and categories of personal data; the categories of recipients of the personal data; details of transfers to third countries including documenting the transfer mechanism safeguards in place; retention schedules; and a description of technical and organisational security measures. The Councils should be documenting what personal data is held, where it came from and who it is shared with. The current form of Information Asset Register in use at the Councils goes some way to address the documentation requirements, although it does not address key details of what personal data is held, where it came from and who it is shared with.	Heads of Service to ensure that information audits are being carried out prior to GDPR implementation to identify all records that contain personal data and document the key details of the processing activities for that data in line with GDPR requirements.	2	*This work, which has been in progress, has also been impacted by the ill health of the Corporate Information Manager and their absence from the office.* *Members of Business Support are assisting service staff to audit their data on shared network drives. As part of this work they are also assisting service staff to ensure the service Information Asset Register is reviewed and updated as required by GDPR in respect of personal data.*	*30/09/2018*	*HoSs*

5	Operational	The GDPR implementation plan provides for a Corporate Privacy Notices Policy to be written by 22 December 2017, with individual departments to subsequently review their existing privacy notices and amend in line with the corporate policy by 28 February 2018. At the time of the audit the corporate policy had not yet been finalised and as such no formal review of privacy notices had taken place within departments. Similarly, the GDPR implementation plan provides for a Corporate Consent Policy to be written by 30 March 2018, with individual departments to subsequently review their existing circumstances of obtaining consent and amend in line with the corporate policy by 24 May 2018. At the time of writing the Corporate Consent Policy had not been finalised.	Corporate Privacy Notices Policy and Corporate Consent Policy be finalised at the earliest opportunity to enable individual service areas to review their existing privacy notices and consent mechanisms prior to GDPR implementation.	2	*This work has also been impacted by the ill health of the Corporate Information Manager and their absence from the office. Other members of Business Support have picked up the work to review and publish updated versions of required documents and these will be published in June* *There will also be additional information available to the public on the websites related to accessing information and data protection.*	*30/06/2018*	*HoBS*

Title of review: **Grounds Maintenance** Date issued: **28 February 2018**

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Compliance	While physical site inspections are carried out, these are carried out as an overall assessment of the condition of a site rather than as an inspection of the specific work scheduled to be carried out by John O'Conner under the grounds maintenance contract. As a result, there is no formal evidence maintained as verification that all scheduled work has been carried out in accordance with the contract. As a mitigating factor, it was accepted that any issues identified relating to grounds maintenance work would be discussed as part of the weekly meetings, however a formal monitoring mechanism should be in place to ensure that work is being carried out in accordance with the standard and frequency as required under the terms of the contract.	Formal monitoring mechanism to be introduced to verify that work is being carried out in accordance with the standard and frequency as required under the terms of the contract.	2	*Noted and plans already in place with a new grounds maintenance contract commencing in April to undertake more detailed and recorded inspections.*	*1st April 2018*	*David Stowe Landscape Assistant*

Title of review: **ICT Network Controls** Date issued: **29 January 2018**

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Compliance	A malicious user attempting to break into a system would typically start by attempting to try to obtain the password for the Administrator superuser account. It is best practice to rename or disable the default Administrator account. A review of superuser access rights on the Chiltern DC domain disclosed that the default 'Administrator' account had not been renamed or disabled.	Management should ensure that default Administrator account is renamed and disabled.	2	*Decision made not to rename administrator account as we have tampered with this in the pass and caused systems to fail. This account is controlled with a 14 character password which only the infrastructure managers knows and a copy of this password is kept in a sealed dated envelope in the safe within Business Support.*	*31.12.2017*	*Frances Phillips (Infrastructure Manager)*
3	Compliance	User account controls within Active Directory offer an administrator the ability to set the 'Password Not Required' flag against individual accounts. If enabled, an account can be set up with a blank password. Audit testing identified 46 accounts where the 'Password Not Required' was set to TRUE. Thus an administrator could set a blank password against these accounts.	Management should ensure that the 'Password Not Required' field is set to FALSE against all Active Directory accounts.	2	*Accepted. This flag was not intentionally set, we believe this may have set itself when accounts where migrated between domains as part of shared services project. A Microsoft PowerShell script was run against AD to reset the flag back to False on all affected accounts.*	*31.12.2017*	*Frances Phillips (Infrastructure Manager)*