tiaa

ICT Audit Report

Audit Committee – 3 July 2014

South Bucks District Council

June 2014

2013/14

ICT Audit Report
June 2014

INTRODUCTION

1. This report identifies the key governance and control issues which currently impact upon the delivery of ICT to both Chiltern and South Bucks Councils. TIAA have undertaken a specific audit of ICT and have identified and prioritised the work which internal audit should undertake during 2014/15 and beyond.

ICT AUDIT PLAN FOR 2014/15

2. As part of the audit review of Chiltern and South Bucks Councils ICT a forward programme of internal audit work has been identified. A copy of the TIAA audit report which includes the 2014/15 ICT audit programme is attached as Appendix A.

KEY RISK OF THE ICT GOVERNANCE AND CONTROLS

3. The Council is undergoing a significant change of emphasis in terms of service delivery and also back office support – in particular ICT support. Without effective management and planning of the ICT function during this change, systems could fail, data security / loss issues could occur, projects slip or fail due to lack of resources or management, changes to applications or operating methodologies may introduce unforeseen errors if not properly managed, staff resources may require changing in terms of skills and expertise, location etc.

4. The findings and outcomes from reviewing this key risk are described in the audit report attached at Appendix A.

Appendix A

tiaa

ICT Governance and Control

Chiltern and South Bucks Councils

March 2014

2013-14

DRAFT

ICT Governance and Control

- EXECUTIVE SUMMARY -

INTRODUCTION

1. We have reviewed the arrangements at South Bucks and Chiltern Councils relating to the ICT Governance and Control arrangements. The review was carried out in March 2014 as part of the planned internal audit work for 2013/14.

SUMMARY

2. The Key Risks identified in the scope for this audit were examined and based on the findings from this work a prioritised ICT audit work stream for future years has been developed. (This is outlined in more detail in Appendix A).

KEY FINDINGS

3. The findings that need to be addressed are largely to agree a prioritised work plan which provides assurances across a range of ICT Governance arrangements in the context of change and the strategic alignment of the two organisations going forward, and to ensure that the service continues to support the organisation's vision and objectives.

RELEASE OF REPORT

4. The table below sets out the history of this report.

Date report issued:	**31 March 2014**

- DETAILED REPORT -

SCOPE AND LIMITATIONS OF THE REVIEW

5. The review examined the governance and control arrangements for the delivery of ICT for Chiltern and South Bucks Councils. This will assist with the ICT audit planning for 2014/15 and beyond. The risks identified in this review are that without proper governance and controls throughout the ICT infrastructure the Council could face ICT disruption and/or corruption to its ICT systems.

6. The limitations and the responsibilities of management in regard to this review are set out in the Internal Audit Annual Plan for 13/14.

7. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. 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. 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.

AUDIT FINDINGS

Key Risk	The Council is undergoing a significant change of emphasis in terms of service delivery and also back office support – in particular ICT support. Without effective management and planning of the ICT function during this change, systems could fail, data security / loss issues could occur, projects slip or fail due to lack of resources or management, changes to applications or operating methodologies may introduce unforeseen errors if not properly managed, staff resources may require changing in terms of skills and expertise, location etc.
Key Controls	The key risk control is that good ICT Governance is demonstrated both currently and during the period of change through strategic leadership and direction across both Councils by means of effective ICT leadership, strategic direction and local management arrangements, robust ICT risk management arrangements, and effective service delivery and performance monitoring plans.

8. The following matters were identified in reviewing the Key Risk Control:

Control 1: ICT governance and strategic management is demonstrated and maintained.

8.1 A Joint Committee has been established comprising representatives of both Councils to provide a strategic lead to joint service provision / delivery and the intended combined ICT support function.

8.2 A Joint Officer Group has been convened to review key work streams going forward in light of decisions made by the Joint Committee.

8.3 A structure has been introduced within ICT which provides a shared ICT management function (Director of Resources & Head of ICT) across both Councils. Within each Authority, the ICT support teams are currently separately provided but there is an intention to converge the two teams.

8.4 As part of our review of the above key control, we identified a number of key areas that are likely to present a risk during the coming months and years and which will require assurance to be provided. These are contained within a suggested ICT audit plan which is shown at Appendix A.

8.5 In order to be sure that we have identified the key areas, we utilised the CIPFA ICT Governance manual contents to ensure that the coverage was complete (this is shown at Appendix B). We have also set our review against a best practice framework defined by COBIT (Control Objectives for IT) provided by the Information Systems Audit and Control Association (ISACA) to ensure that we have reviewed the Councils' ICT governance against an industry standard.

Risk Area 1: IT management and operational arrangements.

9.1 As transformation progresses, there is a need to ensure that the resources are numerically sufficient and also properly configured and aligned to service delivery both during the transition period and as an outcome.

9.2 There are risks that ICT staff see change as a threat, or that they determine that it will ultimately result in fewer staff and may choose to leave. There is also a risk that skill sets do not continue to match requirements going forward.

Risk Area 2: ICT and information risk management arrangements.

9.3 We understand that there is a corporate risk register with a limited number of ICT risks included. There is also an operational risk register which contains more detailed risk assessments.

9.4 For ICT, changes have already started to take place in terms of convergence of systems and applications which is likely to render the risk registers out of date. ICT risks are not considered jointly at this point.

9.5 An Information Governance (IG) Group is in place which will consider some information related risks across both Councils.

Risk Area 3: ICT Strategy development, policies and procedures

9.6 The infrastructure provider for South Buckinghamshire Council (Steria) has been commissioned by both authorities to review infrastructure technology and associated systems at a strategic level. A draft Technology Roadmap has been provided and is under consideration.

9.7 We believe that the whole ICT Strategy, including infrastructure, systems and information should be independently reviewed during their construction and development for both content and coverage, and also to ensure that relevant options have been appraised. Not least because Steria, who are already a service provider cannot provide the independence and objectivity.

9.8 As part of this strategic review we would also include a review of existing policies and procedures in order to establish their preparedness for the future.

Risk Area 4: Management of contractors and third party providers

9.9 As the likely outcome of the transition is a move to greater use of third parties, we believe a vital part of the future for ICT will be contract management. This has also been identified internally as a key area.

9.10 Contract structures, service specifications and also relationship and performance management will be amongst the key areas which we consider to be important and which must have a level of assurance.

Risk Area 5: Programme management and project control

9.11 Aligned to the above, more programmes and projects will be required to be managed. The commissioning function – tenders / quotes etc – is the first stage in any new outsourced arrangement, the controls over which need to be seen to operate to a high standard.

9.12 The formal structure of project management, the associated controls and the standard to which programmes and projects are managed, and their outcomes/benefits realised will also be a key area for management as all too often, projects slip and/or do not meet budget targets (with the resultant savings then jeapordised). There may also be project dependencies which make it critical that they are kept on track.

Risk Area 6: Information security management

9.13 Information security management (ISM) is vital to maintain. Confidentiality, integrity and availability are the cornerstones if ISM and in an environment of change it is essential that the processes which protect data and information, provide resilience and guard against unauthorised access or loss are sound.

9.14 We would expect to look into the processes which protect data and information and also focus on the cross organisational data protections in place including access controls as applications converge. We also believe that education, training and awareness is vital to be maintained ongoing and would expect to determine how the joint arrangements allow/provide for this.

Risk Area 8: Change management

9.15 Again, an area that has been identified internally as one which requires close attention is change management. With a period of significant change already started, the processes which ensure that only authorised changes are properly tested and subsequently made will need to be strong and robust.

9.16 We would expect to review the overall change management process early and also select a significant sample of changes to trace though the process to ensure that nothing is missed during the transformation phase and also that a robust change management system is maintained after transformation is complete.

Risk Area 9: ICT Security structures / access controls / file storage and management

9.17 Access to systems and data, file structures, storage and file management (including retention periods, document marking etc) is another subject area that the Joint Officer Group has on its agenda. It will be important to establish common standards across both authorities if joint working is to be a success.

9.18 There is also a question of unstructured data (word / Excel and other documents) which staff retain either in private folders or on local storage media. Policies for this, and also processes which ensure that it does not become an issue will be essential going forward. There is an associated cost of storage of unstructured data and also the potential for lack of version control.

9.19 There is also the question of adherence to the guidelines for document marking and, again, commonality between organisations.

Risk Area 10: Regulatory compliance

9.20 Compliance (principally) with the Data Protection Act, but also with other legislation as systems, processes, data management functions change will be vital as the councils transition to greater joint working.

Risk Area 11: ICT Quality and performance management

9.21 ICT service quality and performance management is a key ingredient for good ICT management at any time. During such a significant shift in service delivery, the need for this to be maintained is critical. Blame for problems can often be placed at the door of IT sections and/or staff and this must be avoided.

9.22 There is an added factor that the ICT staffs' skills and experience as they exist now, may not be those required some 3/4 years hence as the function evolves. The risk that staff become disillusioned if they fear for their jobs or perceive that their roles are changing or becoming obsolete is something that ICT and the Councils' collective management teams might need to be aware of.

9.23 Maintaining the skills / knowledge and also an appropriate framework for delivery is an area that will need to be tested and verified to ensure that ICT support services are and continue to be fit for purpose.

Risk Area 12: Services provided remotely (cloud)

9.24 There is a significant potential for services to be provided remotely using cloud technology and it is expected that the two councils will increasingly consider these as options. Examples include email and data storage. This in itself has potential for value added such as cost savings, resilience etc. However it also presents a threat as whilst provision along with some risks are transferable (e.g. disaster recovery), other risks are not such as accountability for data security / responsibility for loss.

9.25 We would expect that any transfer of provision to a remote provider to have had certain key considerations made and will test for those as part of the proposed review.

Risk Area 13: Benefits realisation

9.26 The overarching philosophy of sharing, where possible, service delivery mechanisms, and also the back office ICT support function must have real and quantifiable benefits to be a success.

9.27 Our audit review of this area will quantify these benefits and determine from an evidenced baseline that they have been successfully achieved and also that there are no underlying issues such as lack of user take-up, skills, training or awareness.

Risk Area 14: ICT stability during change

9.28 Systems and infrastructure resilience is an area into which an input must be maintained. The ability to continue to provide a service, or quickly recover from an incident is a measure of the resilience of an infrastructure and the prevailing processes e.g. business continuity (BC) & IT Disaster Recovery (ITDR) planning.

9.29 A process which captures and analyses the business impact of changing provision and assesses and quantifies the risks, and feeds this information back to BC/ITDR plans is a significant area – and a significant risk if those information flows break or fail.

9.30 In a changing and resource-constrained environment, there will be an opportunity over the 3/4 year cycle of the proposed plan to ensure that this is maintained and operated to an adequate standard.

Risk Area 15: Public Services Network (PSN) Code of Connection compliance

9.31 There is a review process in place to ensure that compliance is achieved by June 2014. The processes for achieving and maintaining the standards for the code of connection (CoCo) are important.

9.32 In future years, there is a role for internal audit to ensure that the evidence base for maintaining standards – especially during a shift in service provision / delivery – is key. We are able to review the underlying evidence base to ensure that connection to PSN is not jeopardised.

Risk Area 16: Service desk operation

9.33 Maintaining a service desk is essential at all times and particularly so whilst systems, processes, applications and the nature of the provision changes, it will be critical that the service desk maintains up to date details of services. The service desk is often the only interface between users and the actual service provider or between other ICT services such as configuration, release, change and continuity management functions.

9.34 We would expect to review this area to ensure that a customer focused service is being maintained and which meets the needs of the contributing authorities, users and ICT management.

The above areas have been identified as requiring audit attention over the coming 3/4 years. We have prepared an ICT audit plan (See Appendix A) which should form the basis of a discussion with ICT Management in order to prioritise the areas in terms of importance and urgency. The plan document contains columns referenced to the CIPFA IT governance framework to show coverage and also columns for categorising both urgency and importance in order to determine priority. This process will be done in conjunction with ICT management once the plan's contents are accepted.

Appendix A

Audit Plan 2014/15 to 2018/19

Audit Project	Referenced to CIPFA IT Governance Framework (Appendix C)	2014/15	2015/16	2016/17	2017/18	2018/19
Commissioning & Programme Management / Project Control	4	12				8
Management of Contractors & 3rd party providers. (Relationship & Performance, service levels)	2			10		
ICT Strategy, Policies and Procedures (gap analysis, structure, fit with business objectives, development, content and coverage)	1	8				5
Information Security Management in shared service environment (processes, X-organisational data/information protection, X-organisational awareness, training, access to info)	4		10			10
ICT & Information risk management (information risks, compliance, P&P, structures, operational effectiveness – combined risk assessments across both Councils)	2	10		5		

Change management (change management procedures in a transition environment and for the future operating environment)	4	10		5		
ICT Security structures / arrangements / file storage and management (access controls to data and information / file storage / protective ,marking / and retention)	2/4			15		8
Regulatory compliance (DPA / FOI / Other)	4		8		6	
ICT Quality & performance management (skills, experience, knowledge – framework for delivery, service provision & delivery)	4			10		
Control Assurance of services provided remotely (introduction of cloud provision (e.g. data storage / email) – Project Mgt	4		7		10	
IT Management and operational structure (transition and final ICT staffing structures, roles and responsibilities)	2		8			10
Benefits realisation (of transition to shared service deliverer / provider + user take up / usage / skills / experience & training)	4				12	

ICT Stability during changing environment / processes (Resilience & DR & service continuity)	3				12	
PSN Compliance – local aspects from required outputs (compliance review of significant sample of criteria – pre accreditation)	4	5			5	
Service desk operation & management (ensuring that the service desk is established to an appropriate common standard and that users are not disadvantaged or issues unresolved as processes / applications / delivery changes take effect)	4		12			4
Total		**45**	**45**	**45**	**45**	**45**

Appendix B

CIPFA ICT Governance Framework:

Matrix Ref	Subject Area	Relevant To C&SB	Priority	Captured in Forward Work Programme
1	General	limited	3	**N/A**
2	Infrastructure	Yes	2	**Partially**
3	Change Management	Yes	1	**Yes**
4	Configuration Management	Yes	2	**No**
5	System Security	Yes	1	**Yes**
6	Physical and Environmental	Yes	2	**Partially**
7	Service Level Management	Yes	1	**Yes**
8	Operations Management	Yes	2	**Yes**
9	Service Desk, Incident & problem Management	Yes	1	**Yes**
10	Service Continuity Management	Yes	1	**Yes**
11	Cost management	Limited	3	**No**

12	Data Management	Yes	1	**Yes**
13	Performance and Capacity Management	Yes	1	**Yes**
14	Procure IT Resources	Yes	2	**Yes**
15	Project Management	Yes	1	**Yes**
16	Acquisition / Implementation Maintenance of systems	Yes	1	**Yes**
17	Management of 3rd Party Services	Yes	1	**Yes**
18	Education and Training (Users and ICT Staff)	Yes	2	**Yes**

1 = audit input essential

2 = audit input desirable

3 = Not high risk – will keep under review