IT AUDIT NEEDS ASSESSMENT

for

Buckinghamshire Council

July 2021

Martin Baird, Director, Technology Consulting and Assurance (Mazars)

Buckinghamshire Council

CONTENTS

1. INTRODUCTION

We are pleased to present our IT Audit Needs Assessment results and proposed three-year IT audit plan for Buckinghamshire Council. We believe that such an assessment is a vital component of the planning process. It allows IT audits to be focused on areas of risk within the IT environment that are of specific importance to Councils.

Our approach reflects our philosophy that the IT Audit function should be seen as a constructive management tool that provides useful advice to management on the efficiency and effectiveness of systems, procedures and operations. This approach has been successfully introduced across a wide range of our clients, including other Councils.

The following sections give further details of our assessment and the conclusions we have reached.

2. RISK ASSESSMENT APPROACH

In order to identify auditable areas and establish areas of specific importance to the Council, we adopted an approach involving:

- Enquiries with management in Information Communication and Technology (ICT) team and Internal Audit;
- Review of the IT risk register;
- Leveraging our experience across the public sector as well as in Financial Services and Corporates sectors.

The individuals we enquired of include:

Name	Title
Tony Ellis	Service Director ICT
Sarah Barnes	Head of Customer and Governance

This has resulted in auditable areas being classified as either Very High (VH), 'High' (H), 'Medium' (M) or Low (L) risk. Auditable areas of 'Very High' and/or 'High' risk will be reviewed in year 1 and 2 of the three-year audit cycle. Those areas of 'Medium' risk will be reviewed in subsequent years. Table 1, in Section 3: Proposed Audit Plan for 2021/2022 to 2023/2024, summarises the auditable areas identified and their associated risk.

3. PROPOSED IT AUDIT PLAN FOR 2020/2021 TO 2022/2023

Table 1: Audit areas identified through the IT Audit Needs Analysis

AUDITABLE AREA	Risk Level	2021/2022 Days	2022/2023 Days	2023/2024 Days
Cyber Security	**H**	15		TBC
IT/Infrastructure Resilience	**H**	20		
Disaster Recovery and Backups	**H**	20		
IT Service Provider/Contract	**M**		20	
Data Centres/Cloud Controls	**H**		20	
Change/Patch Management	**H**	20		
Application Management/Governance	**M**		15	
Total		**75**	**55**	**0**

Note:

The above only addresses the audits proposed and does not include other auditable areas that are possible. In section 5 below, we have provided some comparisons/insight from our experience with other LG clients in the last 12 months to provide other suggestions that could be included in the plan.

4. ANNUAL IT AUDIT ACTIVITY PLANS

Table 2

Annual IT Audit Plan 2021/2022		
AUDITABLE AREA	**Risk**	**Days**
Disaster Recovery and Back-ups	**H**	20
IT/Infrastructure Resilience	**H**	20
Change/Patch Management	**H**	20
Cyber Security	**H**	15
Total		**75**

The above extract (Table 2) from the IT Audit Needs Analysis (Table 1) shows areas that have been identified for review as part of the 2020/2021 Audit Plan. The following summarises the rationale and focus for each of these audits:

Disaster Recovery and Backups

Disaster recovery was noted as having a residual risk score of 10 in the Council's IT risk register with a fully tested strategy and plan required to provide the Council assurance that full business continuity can be provided.

Disaster Recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. IT Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events.

Given the COVID-19 pandemic, it is even more critical that disaster recovery strategies and plans are regularly reviewed, updated and tested, including the need to ensure emerging scenarios such as the pandemic are included.

In addition, without an effective backup regime and one that ensures that offline copies are retained (to reduce the risk of malware infection in the case of London Borough of Hackney), an organisation is not likely to be able to effectively and efficiently recover in a disaster scenario. Therefore, this audit would also test controls in regard to backup scope, frequency, offsite location, testing and recovery.

IT/Infrastructure Resilience

A number of IT/Infrastructure resilience-related risks feature in the Council's IT Risk Register, including:

- Cyber Security – which refers to the lack of resilience of systems as part of the description.
- Disaster Recovery – as per 'Disaster Recovery and Backups' above.
- Updata Contract Transition – which refers to the fact that if the Council is not able to manage the contract transition to new providers before the Updata contract terminates, then service stability and performance cannot be assured, leading to a failure in key services (e.g. N Drive, SWIFT, SAP, Outlook).
- Legacy Data Centre at Amersham and Wycombe – refers to the risk that if the legacy data centres are not fit for purpose, then there may be an issue with the resilience of key services.

Recent application IT controls reviews of systems such as K2, Respond, and Routewise identified 'system resilience and recovery' as a shared risk/theme arising across applications and supporting infrastructures.

This audit will address the following:

- COVID-19 Lessons Learned – consideration of the impact of the pandemic on IT/infrastructure resilience, the remediation of problems due to a rapid shift to remote working and the building upon any identified good practices to support service improvement.
- People, process and technology perspective, including a high-level review of the IT architecture and technology in place.
- Linkage/alignment to DR and BCP processes (as above).

Change/Patch Management

The Council is currently seeking to deploy upgrades to the IT service management system and further enhancements to the existing change control process. Linked with these enhancements, IT plans to use ServiceNow for the Configuration Management Database (CMDB). The CMDB will link to IT service management areas such as change, incident/problem management and asset management.

This audit will therefore address the following:

- Change to infrastructure and applications are governed through a consistent policy/process;
- The change process addresses the request, impact, authorisation, testing, deployment of changes;
- Comparison with LG peers concerning good change control practice commonly identified;
- Patch management is undertaken across the estate in a complete, accurate and timely manner.

Cyber Security

The IT Risk Register includes a Cyber Security risk which has a current risk score of 12. If the Council's Cyber Security processes are not communicated effectively and the systems are not robust then there will be an increased risk of significant damage to the Council's data/systems from cyber attacks. In addition, having to manage disparate IT environments which are then brought together could make the Council vulnerable to threats that do not currently exist leading to loss of data, breach of data and denial of access.

A Cyber Security audit is scheduled to be completed as part of the 2020-21 audit plan. However, it is being conducted during September 2021 onwards. Given the importance of Cyber Security and the associated risks, a follow-up of the 2020-21 audit should be planned.

Table 3

Annual IT Audit Plan 2022/2023		
AUDITABLE AREA	**Risk**	**Days**
IT Service Provider/Contracts	**M**	20
Data Centres/Cloud	**H**	20
Application Management/Governance	**M**	15
Total		**55**

The above extract (Table 3) from the IT Audit Needs Analysis (Table 1) shows areas that have been identified for review as part of the 2022/2023 Audit Plan. The above is based on the current assessment of risks and is therefore subject to change. The following summarises the rationale and focus for each of these audits:

IT Service Provider/Contracts

The Council's IT Risk Register includes a risk regarding the 'Updata Contract Transition', which albeit not assessed as a high risk, enquiry of management informed that service stability and performance cannot be assured if the Council is not able to manage the contract transition to new providers before the contract terminates. This review will focus on the following high-level areas:

- Service Scope/Alignment – review of current contracts and service agreement to determine alignment with Council business requirements.

- Risks and Controls – testing of key processes and controls supporting the specific contract/service agreement, mapping of relevant certifications/accreditations provided by the 3rd party IT provider (e.g. ISO27001, SOC1, SOC2, ISAE3402).
- Reporting and Governance – review of service level management reporting processes and controls, whether the reporting addresses the specified contract/service agreement in place and management challenge of the provision.

Data Centres/Cloud

The Council's IT Risk Register includes a number of relevant risks concerning data centres, including (a) Legacy Data Centre at Amersham – this risk specifically relates to perceived environmental security risks and (b) Legacy Data Centres at Amersham and Wycombe – this risk specifically relates to perceived risks of the data centres not being fit for purpose leading to risks about the resilience of key systems and infrastructures.

Depending on the requirement, this audit could address the following:

- The Physical and Environmental Controls supporting the existing Council data centres.
- A similar or combined scope as per the IT Service Provider/Contracts audit (as above).

Application Management/Governance

We have noted many common risks and themes arising from reviews of K2, Respond and Routewise. We plan to undertake an IT application audit of the recently implemented LiquidLogic Adults' Social Care System (LAS) application. It is feasible that the common themes from previous application audits as follows may be relevant:

- System resilience and recovery;
- Application management and governance;
- System security.

This audit would focus on following up on the themes arising from previous audits, specifically regarding 'application management and governance' and on this theme for a sample of other applications not previously reviewed.

5. COMPARISON WITH PEERS/EXPERIENCE

Mazars Technology Consulting & Assurance team audit a wide range of Local Government clients across the UK; therefore, we can leverage the knowledge of your peers as well as our experience across the Public Sector, Financial Services and Corporates sectors.

Set out below is our observations from the above experience for consideration for inclusion in the annual IT audit plans:

Theme	Context
DSP Toolkit	The Council's risk register includes a risk "NHS Data Sharing" and cites in the risk description "If IT are not able to provide enough assurance for the NHS Toolkit, then data sharing may not be possible". We commonly provide DSP Toolkit audits for NHS IA clients but are now more commonly being asked for the same for those organisations that work with the NHS (including Local Government and Charities for example). We usually deliver these audits with a mixed team of IT audit and Data Privacy specialists.
Data Analytics/Curious	We have recently discussed (with other LG IA clients) the feasibility of utilising our Curious data analytics tool (developed in-house) to support the audits of key business processes. Commonly the trigger for these discussions is cost pressures imposed on Internal Audit, which have resulted in the need to provide more substantive assurances with less audit days and the increasing demand for automation in audit and reducing the reliance on manual testing of controls.
Independent Project Assurance	We noted that with the creation of Buckinghamshire Council, IT are bringing together four sets of IT infrastructure, multiple business systems, data and processes. Although a single Email system project has been delivered, the IT services continue to be delivered across highly fragmented environments. The ICT ONE Programme is intended to bring these together to provide staff with a single consistent quality IT environment and to facilitate the Council's transformation. We have undertaken independent programme and project assurance for similar transformations both in the public sector and across other sectors in the UK.
IT Strategy	Given the Council itself and as a result, IT have undertaken significant changes/transition, much of the transition is likely to influence changes to the strategic direction in regard to Council IT. Assurances can be (a) provided pre-implementation of the IT strategy to support the development of the document and the framework for delivery or (b) post-implementation to identify any gaps based on peer comparison and best practice.

IT Service Management (ITIL)	Comparison with your peers' highlights that many Councils are transforming their IT operating model as part of cloud adoption, reliance on 3rd parties and commonly because budgets have been constrained and reduced further. Whether the IT service is inhouse or reliant on a 3rd party, we commonly undertake IT Service Management reviews using ITIL as the framework.