MAZARS

CROYDON

Final Internal Audit Report

Members - Bring Your Own Device (BYOD)

August 2017

Distribution:

Executive Director Resources (Final only)

Director Customer & Corporate Services

Head of ICT and Transformation

ICT Service & Contract Manager

ICT Business Partner Manager

Head of Risk & Corporate Programme Office

ICT Technology & Architecture Manager

Head of Democratic Services and Scrutiny

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	2
	Priority 3	1

Status of Our Reports
This report ('Report') was prepared by Mazars Public Sector Internal Audit Limited at the request of the London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, we have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of the London Borough of Croydon and to the fullest extent permitted by law, Mazars Public Sector Internal Audit Limited accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility set out in appendix 3 of this report for further information about responsibilities, limitations and confidentiality.

Contents

Page

Executive Summary

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 Bring Your Own Device (BYOD) refers to the policy of permitting employees (and Members) to bring personally owned mobile devices (laptops, tablets and smart phones) to their workplace, and to use those devices to access privileged Council information and applications. At the time of audit the BYOD arrangements were restricted to Council Members only. As the Council is required to deliver significant budget savings, the opportunity has been taken to identify alternative ICT provision for Members that provides financial savings and greater flexibility and agility for Councillors, hence BYOD. It should be noted that the implementation of Members BYOD was done as a separate project and the Council is working on rolling out a separate BYOD project for the rest of the Council staff. The IT management is fully aware of the scale of implementation of Members BYOD and its limitations. Considering that the Members do not access many parts of the Council's network and systems, more ground work is still to be done for the entire staff BYOD implementation.

1.2 This audit is part of the Internal Audit Plan for 2016/17. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Recommendations
The Members BYOD policy documentation should be compounded into one comprehensive policy clearly showing approval, key terms and user acceptance, **(Rec 1).**
There were ongoing negotiations with Capita at the time of audit to change the contractual arrangements for supporting the Members IT. These need to be finalised and implemented. **(Rec 2).**

The Priority 3 recommendation is detailed under item 4.

3. Actions and Key Findings/Rationale

BYOD Policy: Creation of a comprehensive Members BYOD Policy.

Priority	Agreed Action/s (Recommendation 1)	Detailed Finding/Rational
2	A comprehensive Members BYOD policy should be created. This can be done by combining all existing BYOD usage guidance documentation. This policy should be ratified and should require users to sign an acceptance clause.	A comprehensive policy ensures that all Members are aware of their usage responsibilities and can be held to account. The transition from Council issued devices to Members own devices has not been clearly reflected in the policy documentation. While there used to be a comprehensive Mobile Device Acceptance Form and Usage Policy, which focused on Council issued devices, the same cannot be said for the Members BYOD policy arrangements. Although there are BYOD usage documents, such as management reports and guidelines, Audit could not clearly establish the policy approval, Member acceptance and future review arrangements. Where a comprehensive policy is not in place, Members may not be aware of their responsibilities and there could be unauthorised disclosure of Council data which could negatively affect the Council's reputation.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
This is being undertaken in conjunction with the LBC staff BYOD policy. A BYOD Policy has been signed off and a draft of the new computers for councillor's policy has been produced. This policy is expected to be finalised and approved by 31st August 2017.	Agreed	IT Commercial Manager	31st August 2017

Technical and User Support:

Priority	Agreed Action/s (Recommendation 2)	Detailed Finding/Rational
2	Management must ensure that BYOD related contractual changes and Service Level Agreement (SLA) with Capita are finalised and implemented. Any work in progress should be prioritised and expedited.	The introduction of Members BYOD results in a reduction to the support services Capita is contracted to provide to Members and also results in a change to the existing SLA to provide support to Members, i.e. Members are now required to seek first line support from service providers other than Capita. However, Capita are still required to provide support for the technical aspects for access to Council services. It was established that negotiations with Capita to change the contractual arrangements and SLA for supporting Members IT resulting from the introduction of Members BYOD were ongoing at the time of audit. Where the contractual arrangements are not finalised, there is a risk that the Council may be paying for services no longer required. Where a support SLA is not in place, support performance is difficult to monitor and additionally, Members might not get the support services that the Council is paying for.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
A review of the Members support within the contract has already been discussed and agreed by LBC & Capita. A reduction in the service charges paid for this particular service will come into effect by the end of July 2017. Support for business application related issues will continue to be covered by the current SLA's in place with Capita. However, there will be no new SLA's put in place for covering BYOD at this time.	Agreed	ICT Service & Contract Manager	31st August 2017

4. Priority 3 Recommendation

Agreed Action/s	Detailed Finding / Rationale
1. Management should ensure that the Technology Risk Register is refreshed to include BYOD related risks.	While a Risk Assessment was carried out, the Council Technology Risk Register has not been refreshed to include BYOD related risks. Where the Technology Risk Register has not been refreshed to include BYOD risks, the initial risk assessment results could be ignored and risks might go unmanaged until they materialise.

Appendix 1

TERMS OF REFERENCE

Members Bring Your Own Device (BYOD)

1. INTRODUCTION AND BACKGROUND

1.1 Bring Your Own Device (BYOD) refers to the policy of permitting employees (and Members) to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged Council information and applications. The current BYOD arrangements are restricted to Council Members. This audit is part of the Internal Audit Plan for 2016/17 as agreed by the General Purposes and Audit Committee.

2. OBJECTIVES AND METHODOLOGY

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of the control environment operating for the Internal Network.

2.2 In order to achieve the overall objectives, a risk based systems audit approach will be carried out, documenting and evaluating the actual controls against those expected and based on this, undertaking appropriate audit testing.

2.3 The key findings, conclusions, and subsequent recommendations arising will be discussed with management at an exit meeting, followed by the circulation of a draft report for consideration, prior to agreement and issue of the final audit report.

3. SCOPE

3.1 This audit examined the following areas:

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Risk Management	0	0	1
Policy	0	1	0
Legal Issues	0	0	0
Technical and User Support	0	1	0
Governance	0	0	0
Training	0	0	0
Mobile device Layer Security	0	0	0
Mobile Device Management	0	0	0

Appendix 2

DEFINITIONS FOR AUDIT OPINIONS AND RECOMENDATIONS

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

🟢	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are consistently applied.
🟡	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk.
🟠	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
🔴	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

Priorities assigned to recommendations are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represent an exposure to risk and require timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

Appendix 3

STATEMENT OF RESPONSIBILITY

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars Public Sector Internal Audit Limited accepts no responsibility and disclaims all liability to any third party who purports to use or reply for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.