MAZARS

CROYDON

Final Internal Audit Report

Mobile ICT Devices

December 2016

Distribution: Executive Director of Resources (Final only)
Director of Customer and Transformation
Head of Transformation
ICT Service & Contract Manager

Assurance Level	Recommendations Made	
Limited Assurance	Priority 1	0
	Priority 2	6
	Priority 3	2

Contents

Page

Executive Summary

1. Introduction

Mobile ICT devices principally include laptops, tablets and smartphones and are increasingly used for greater productivity and flexibility to achieve the Council's objectives. The risks associated with the use of ICT mobile devices includes:

- Weaknesses in the security and resilience of mobile ICT devices with potential loss to ICT systems, data confidentiality and availability; and
- Inadequate asset management and security monitoring resulting in potential loss of devices and to data security.

This audit is part of the Internal Audit Plan for 2015/16 as agreed by the General Purposes and Audit Committee. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Recommendations
ICT Security and related policies are not up to date **(Rec. 1).**
Asset register maintenance and reviews are not adequate **(Rec 2).**
Responsibilities for Mobile Device Asset Management are not clearly assigned **(Rec 3).**
Facility on smartphones to block the installation of unauthorised software not activated **(Rec 4).**
Production of Management Reports not being carried out **(Rec5).**
Devices Disposal Records and Procedures are not adequate **(Rec 6).**

Priority 3 recommendations are included under item 4.

3. Actions and Key Findings/Rationale

IT Strategy, Information Security (IS) and Acceptable Usage Policies: IT Security Policy, Standards and Guidelines are adequate.				
Priority	**Agreed Action/s (Recommendation 1)**	**Detailed Finding/Rational**		
2	Management should ensure that all security related policies are updated at least on a yearly basis. The following policies need updating: • ICT Infrastructure Policy; • ICT Equipment Allocation Policy; • IT Access Policy; • Information Protection policy; • ICT Acceptable Usage Policy and Personal Commitment Statement; and • HR Information Security Policy.	Updating policies regularly is done to ensure that they remain relevant and fit for purpose. Only up to date policies can be used to uphold the Council's values and maintain its priorities. During the audit, we discovered that all the ICT security related policies have not been updated for a number of years. An example was the IT Equipment Allocation Policy which has details of Blackberry devices which are being phased out, but it does not include any information on new devices such as Windows phones that have been introduced. We noted that there is work in progress to update these policies. The risk of having outdated policies is that formulating and enforcing regulations will be impossible or difficult if the endorsed policies do not have necessary information to support the regulation process. Regulations made outside policy in this case might not be legally binding.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
As part of the overall ICT Policies Review, these policies along with others are currently being reviewed and updated with the EoW programme.		Agreed	ICT Service & Contract Manager	December 2016

Inventory Recording and Asset Numbering: All mobile device assets are updated to the IT asset register/inventory database.				
Priority	**Agreed Action/s (Recommendation 2)**	**Detailed Finding/Rational**		
2	Management should ensure that the asset registers are accurate and maintained up to date. Asset registers should be regularly reviewed and reconciled to ensure their accuracy.	Up to date asset registers give a correct record of the Council's mobile device assets at any given time. Accountability is easy to enforce where asset registers are up to date. The periodic review of asset registers ensures accuracy, completeness and minimises asset losses. During the audit we discovered that the mobile assets registers were **not** up to date, providing an accurate record. In particular: • For smart/mobile phones two asset registers are maintained for the same devices, one by the Council and another by Capita therefore duplicating. These registers were not in sync with discrepancies of devices recorded on one and not the other; and • For smart/mobile phones, tablets and laptops, records were found to be incomplete with key information missing, for example, not assigned to named users, serial numbers and International Mobile station Equipment Identity (IMEI) numbers. There are also no regular reviews and reconciliations of the mobile assets registers by either the Council and/or Capita. An outdated asset register overstates or understates the Council's mobile devices asset inventory at any given time. If registers are not up to date, user accountability is adversely affected. Lack of regular reviews and reconciliation could lead to asset losses going on undetected together with data loss.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
The asset register for mobile devices is held centrally on SharePoint by means of a spread sheet. Gaps within the register at the time were down to transition information which was never forthcoming. This should now be resolved. As part of monthly CMDB checks, LBC now review a		Agreed	ICT Service & Contract Manager	December 2016

sample of devices within the spread sheet and compare this with the leavers report to ensure this list is up to date.			

Inventory Recording and Asset Numbering: Responsibility for mobile device asset management should be designated.			
Priority	**Agreed Action/s (Recommendation 3)**	**Detailed Finding/Rational**	
2	Responsibility for the Council's mobile device asset records management should be defined, documented and formally designated.	Clearly defined roles and formal assignment of responsibilities will help ensure that the Council's ICT mobile assets are adequately managed and accounted for. Clear service level agreements ensure that the Council is getting the right services as per their needs. SLA also gives the Council a mechanism by which to monitor the performance of the service provider. During the audit, we established that the responsibility of managing mobile devices has been transferred as part of the contract to Capita. Only the order processing of mobile phones remains with the Council. The Council still maintains a copy of the mobile phone register. Capita uses the MobileIron Mobile Device Management (MDM) application to maintain a register of the mobile phones. What was not clear is how the mobile phones, which are not compatible with MobileIron MDM are going to be managed. We examined the Mobile Device Asset Management element of the Contract between the Council and Capita and found it contained no defined service levels. Failure to clearly define, document and formally assign the roles and responsibilities for managing the Council's mobile asset records increases the risk that clear guidance will not be available and control over the function will be weakened as a result. This may also lead to poorly coordinated mobile asset management activities. A contract without clearly defined service levels may mean the Council is not aware that they are not receiving the standards of support that have been procured.	
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
Capita are now fully responsible for the management of Mobile Devices and ordering of these devices. All devices whether		Agreed	ICT Service & Contract Manager	TBA

they be Smartphone/Mobile should be recorded and maintained in the CMDB spread sheet.			

Security and Configuration of Mobile Devices: Unauthorised software is identified.				
Priority	**Agreed Action/s (Recommendation 4)**	**Detailed Finding/Rational**		
2	Management should ensure that a list of unauthorised software is created and maintained and these are blocked by the MDM software.	Restricting installation of unauthorised application on the Council's mobile devices reduces the prevalence of malicious programs that could potentially steal data. During the audit, we established that the facility on smartphone devices to block unauthorised software exists, has been tested but not activated. Having unrestricted application installations on the Council's mobile devices exposes the Council's network to spyware and other malicious programs such as Trojans. This could result in the Council's data being illegally accessed.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
A senior management decision was made to allow as much flexibility as possible on the use of the devices and downloading of applications. This was reviewed and agreed by Information Management at the time of the rollout and no issues were raised. Whilst there is a potential for loss of data, it is deemed at this time as being low risk.		Disagreed	ICT Service & Contract Manager	N/a

Mobile Device Monitoring and Reporting: Adequate management reports are produced for monitoring and ensuring compliance with policies.

Priority	Agreed Action/s (Recommendation 5)	Detailed Finding/Rational
2	The Council should ensure that compliance and inventory reports are produced on mobile assets. Reports should be provided in pre-defined formats and produced on regular basis or as when needed.	Reports are a management tool that provides the basis for making decisions. The most useful reports are those provided in a predefined format and available as when needed. During the audit, we established that compliance and inventory reports were yet to be produced from the MDM application managing smart phones. The Council's asset management staff found not to have access to any records for Laptops and Tablets held by Capita. If reporting is not done accurately and timely, the quality of decisions made by managers is adversely affected. Without proper reporting, enforcing accountability and compliance is difficult.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
LBC now receives a monthly Mobile Iron report from Capita which allows the Asset information to be reviewed and inventoried to ensure records are accurate and highlight any issues in consultation with the monthly leavers report.	Agreed	ICT Service & Contract Manager	December 2016

Asset Loss Management Procedures: Adequate Mobile Device Disposal procedures are in place.				
Priority	**Agreed Action/s (Recommendation 6)**	**Detailed Finding/Rational**		
2	The Council should have a formally documented mobile devices disposal guidelines and procedures. All relevant details about a disposed asset should be recorded in the asset register, for example, date of and reason for disposal. Any disposal should be approved by management.	Formally documented disposal procedures ensure that only devices earmarked for disposal are disposed. These procedures will also ensure that all disposed devices are wiped clean and do not contain any data belonging to the Council. During the audit, we established that there were no formal disposal procedures in place. The recording of disposal of mobile assets in the asset register did not give enough detail about the disposal, for example, disposal date and reason. If the disposal of mobile devices is not guided by procedures, the Council's data held on disposed devices might be viewed by unauthorised personnel which could result in action under the Data Protection Act by the Information Commissioner. A lack of disposal guidelines might result in disposal of some devices which can still be used.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
LBC are working with "Go On Croydon" & we have signed an asset disposal agreement with a company called "computer recyclers". This company will take all our equipment and dispose of it within WEEE legislation and also ensure that CESG approved standards are used. However, for laptops/desktops, where they can they will recycle and donate a number of devices back to LBC to distribute to local community groups. Some of the other devices can then be purchased from this provider for a nominal fee (e.g. £20).		Agreed	ICT Service & Contract Manager	Complete

4. Priority Three Recommendations

Recommendation	Rationale
1. Management should ensure that a new ICT strategy is formulated and documented. This should include new ways of working and emerging technologies.	An ICT strategy contains the Council's ICT strategic vision and how it can be achieved. It also details key network and infrastructure aspects to achieve the vision including those on mobile devices, and the relevant technical standards that will be applied. The ICT strategy is a basis for steering all ICT projects. During the audit we found that the Council's five year ICT strategy expired in 2014. No explanation was given as to why this has not been updated, although we were informed that all ICT polices are currently being reviewed. We were informed that the Council is considering the introduction of Bring Your Own Device (BYOD) as a new way of working. There are currently security issues with BYOD but these will be overcome with the introduction of Citrix. Without an ICT strategy, the Council is not in a position to tell how many ICT projects they can accommodate in a specified period of time including those for mobile devices and this can result in under or over allocation of resources.
2. There should be a clear link between the logged helpdesk calls for lost or stolen ICT devices and the recording in the asset register.	Keeping a complete and detailed record for lost devices is useful when it comes to tracking the devices, processing insurance claims and enforcing accountability. During the audit we found that whilst there were records of equipment losses, some of the records have missing details for these devices. For example, given details for the asset loss record did not have any reference or link to the help desk call documenting the loss incident. Warrant information records were not available for some devices in the asset register. If records for losses of equipment are incomplete or lack specific detail, processing insurance claims and tracking the devices might be difficult.

Appendix 1

TERMS OF REFERENCE

Mobile Devices Audit

1 INTRODUCTION

1.1 As part of the agreed 2015/2016 Audit Plan for the London Borough of Croydon, an audit is due to take place regarding the control environment for Mobile Devices.

2 OBJECTIVES AND METHOD

2.1 Our audit objective is to provide an objective independent opinion on the adequacy and effectiveness of the control environment with regards to Mobile Devices.

2.2 In order to achieve the objectives, a risk based systems audit will be conducted.

2.3 The findings, conclusions, and subsequent recommendations arising therefrom will be presented at an exit meeting to be arranged with the auditee. Following the exit meeting, a draft report will be issued encompassing the auditee's initial comments. In accordance with the Council's audit reporting Protocol, ten (10) working days will be allowed for a formal response to the draft report.

2.4 Upon receipt of the formal response or ten (10) working days after the issue of the draft report, whichever is sooner, a final report will be issued.

2.5 A follow up audit will be conducted at an appropriate point in the future, to provide assurance on the implementation of any recommendations made in the final report.

3 SCOPE

This audit examined the following areas:

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Information Security and Acceptable Use Policies	0	1	1
Staff Education, Training and Security Awareness	0	0	0
Mobile Device Asset Management Policy	0	0	0
Inventory Recording and Asset Numbering	0	2	0
Security and Configuration of Mobile Devices	0	1	0
Mobile Device Monitoring and Reporting	0	1	0
Asset Loss Management Procedures and Processes	0	1	1

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 for this report which is prepared on the basis of the limitations set out below.

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. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by us should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all 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. Our procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our work and to ensure the authenticity of such material. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Mazars Public Sector Internal Audit Limited

London

December 2016