MAZARS

CROYDON

Final Internal Audit Report

Windows Operating System Security

August 2017

Distribution:

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

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	1
	Priority 3	4

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 The Council's network infrastructure, including server operating system security, is managed by its IT service provider, Capita. As part of this year's plan, an internal audit in respect of the Windows Operating System for a key system in use by the Council, namely MobileIron hosted on a Microsoft Windows 2012 server build, was identified to be undertaken as a sample of the security configuration applied to the operating system.

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 Issues
[redacted] (Rec 1).

Priority 3 recommendations are detailed under item 4.

3. Actions and Key Findings/Rationale

<table>
<tr><td colspan="5"><b>Updates and Patches:</b> Security Updates and Patches</td></tr>
<tr><td><b>Priority</b></td><td><b>Agreed Action/s (Recommendation 1)</b></td><td colspan="3"><b>Detailed Finding/Rational</b></td></tr>
<tr><td>2</td><td>[redacted]</td><td colspan="3">[redacted]</td></tr>
<tr><td colspan="2"><b>Management Response</b></td><td><b>Agreed/Disagreed</b></td><td><b>Responsible Officer</b></td><td><b>Deadline</b></td></tr>
<tr><td colspan="2">[redacted]</td><td>Agreed</td><td>Service Delivery Manager
Capita IT Enterprise Services</td><td>31st August 2017</td></tr>
</table>

4. Priority 3 Recommendations

Agreed Action/s	Detailed Finding / Rationale
1. Management should reduce the Lockout Threshold duration setting in the Account Policy from the current setting [redacted].	The analysis of the Account Policy settings on the MobileIron Windows Operating System identified that the Lockout Threshold (i.e. invalid password attempts) has been set to [redacted]. It is accepted that at present there is only one account on the system and that is the Administrator Account. Where account policies are weak, there is a risk of unauthorised access attempts.
2. Management should ensure that the Audit Policy settings on the MobileIron Windows server are enhanced by configuring the following suggested settings: [redacted] [redacted]	The analysis of the audit policy settings identified that although auditing has been set for [redacted], it has not been set for [redacted] [redacted]
3. Management should ensure that the Discretionary Access Control Lists (DACLs) are reviewed to ensure they are valid, current and that permissions granted through them are appropriate.	[redacted] [redacted]
[redacted] A review of the services and drivers installed on the server should be undertaken [redacted]	[redacted] [redacted]

[redacted]	[redacted]

Appendix 1

TERMS OF REFERENCE

Windows Operating System Audit

1. INTRODUCTION AND BACKGROUND

1.1 The Council's network infrastructure, including server operating system security, is managed by its IT service provider, Capita. As part of this year's plan, an internal audit in respect of the Windows Operating System for a key system in use by the Council – MobileIron hosted on a Microsoft Windows 2012 server build, was identified to be undertaken as a sample of the security configuration applied to the operating system.

1.2 The scope of this audit will look at the configuration of the security policies in the Windows Operating System with the aid of the SekChek security analysis tool.

1.3 This audit is part of the agreed Internal Audit Plan for 2016/17.

2. OBJECTIVES AND METHODOLOGY

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness control framework operating

2.2 In order to achieve the overall objective, 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 testing. Comparison will be made as appropriate with best practice guidance.

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, (as these relate to Windows OS Security):

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
System-wide Security Policies	0	0	1
Audit Policy Settings	0	0	1
Event Logs Settings	0	0	0
Registry Key Security Options Settings	0	0	0
User Accounts and Passwords	0	0	0
Rights and Privileges	0	0	0

Trusts and Remote Access	0	0	0
Services and Drivers	0	0	1
Logical Drives and Network Shares	0	0	0
Updates and Patches	0	1	0
Discretionary Access Controls	0	0	1
Default Accounts	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.