

Final Internal Audit Report

Windows 10 Gold Build Desktop Security

August 2017

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

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

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

1. Introduction.....	2
2. Key Issues.....	2

Detailed Report

3. Actions and Key Findings/Rationale	3
---	---

Appendices

1. Terms Of Reference
2. Definitions Of Audit Opinions And Recommendations
3. Statement Of Responsibility

1. Introduction

- 1.1 Windows 10, is the latest operating system (OS) from Microsoft which Capita, the Council's IT Service provider, is rolling out to the Council's virtual desktop estate solution as part of its technical refresh programme.
- 1.2 The roll out was initially piloted through a small number of desktops from around the middle of this year and at the end of the audit in September, the Council had nearly 1500 devices/machines with the new Windows 10 OS.
- 1.3 As part of the audit, two security assessment tools were used to analyse the configuration settings applied on a sample Windows 10 Desktop. These tools were Belarc Advisor (8.5.3 – for Windows 10) and the PC Auditor tool from SekChek.
- 1.4 The General Purposes and Audit Committee agreed the Internal Audit Plan for 2016/17 on the 23 March 2016. As part of that plan, an internal audit in respect of the Windows 10 Gold Build Desktop Operating System was identified to be undertaken.


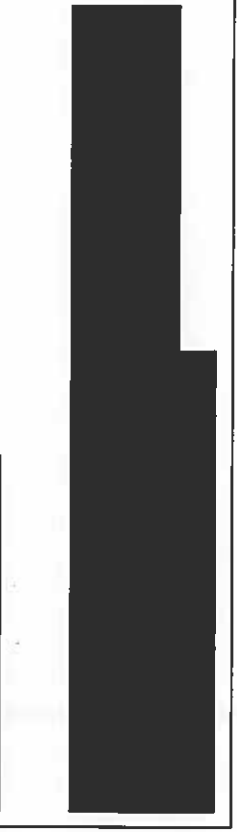
2. Key Issue

Priority 2 Recommendation

(Rec 1).

3. Actions and Key Findings/Rationale

<u>Control Area 2: Technical Security Configuration Settings</u>			
Priority	Recommendation 1	Detailed Finding / Rationale	
2	[Redacted]	Addressing or undertaking a sample review will help ensure that the configuration applied to the desktops is in line with agreed standards and Council requirements.	
	[Redacted]	[Redacted]	[Redacted]
	[Redacted]	[Redacted]	[Redacted]
<u>Management Response</u>			
	[Redacted]	Agreed/Disagreed	Deadline
	[Redacted]	Agreed	Completed
	[Redacted]	Responsible Officer	ICT Service and Contract Manager

				
---	---	--	--	--

TERMS OF REFERENCE

Windows 10 System Security

1. INTRODUCTION

- 1.1 The Council's IT Services is provided by Capita, its IT service provider. As part of a technical refresh, the Council is currently in the process moving to a virtual desktop solution that includes the roll out of the latest Microsoft Desktop operating system Windows10.
- 1.2 This audit is part of the agreed 2016/17 Internal Audit Plan and will examine the configuration settings applied to the Windows10 Desktop operating system.

2. OBJECTIVES AND METHODOLOGY

- 2.1 The overall audit objective of this audit is to provide an objective independent opinion on the adequacy and effectiveness of controls and processes established and applied to the management and use of Windows10 security features.
- 2.2 The audit will use a range of appropriate security assessment tools to analyse the configuration settings applied on a sample Windows 10 Desktop. These tools include Belarc Advisor (8.5.3 – for Windows 10) and the PC Auditor tool from SekChek. The Microsoft Security Baseline Analyser may also be used, if it has been updated to include Windows 10 by the start of the audit.
- 2.3 For each of the control and processes in the scope below the audit will:
- Walkthrough the processes to consider the key controls;
 - Conduct sample testing of the identified key controls, and
 - Report on these accordingly.
- 2.4 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 will examine the Council's arrangements for controlling the Hyperion application:





Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Security Standards and Procedures	0	0	0
Technical Security Configuration Settings	0	1	0

System Management Trails	0	0	0
System Support Arrangements	0	0	0

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.

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 rely 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.