

# Final Internal Audit Report

## Antivirus and Malware

### August 2017

**Distribution:** Executive Director Resources (Final only)  
 Director Customer and Transformation  
 Head of ICT & Transformation  
 Information & Systems Manager  
 ICT Service & Contract Manager  
 Head of Insurance, Risk and Corporate Programme Office

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

#### Status of Our Reports

This report ("Report") was prepared by Mazars Public Sector Internal Audit Ltd at the request of 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 Internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit 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 London Borough of Croydon and to the fullest extent permitted by law Mazars Public Sector Internal Audit Ltd. 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 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

---

### Appendices

1. Terms of Reference
2. Definitions of Audit Opinions and Recommendations
3. Statement of Responsibility

## **1. Introduction**

- 1.1 Antivirus software is a key component of every organisation's defence against the threats posed by malicious software ('malware' - e.g. viruses, computer worms and ransomware).
- 1.2 Antivirus software attempts to prevent the installation of known malware, as well as identifying and removing any threats identified on an organisation's computers or wider infrastructure.
- 1.3 The Council employs two antivirus solutions, one for servers / infrastructure (Symantec Endpoint) and one for end-user devices (Microsoft Windows Defender). It is important that both solutions are kept up-to-date with the newest virus definitions and software updates. In addition, the regular patching of servers and end-user devices with the newest Microsoft security fixes ensures that known security weaknesses are not exploited.
- 1.4 The General Purposes and Audit Committee agreed the Internal Audit Plan for 2017/18 on the 22 March 2017. As part of that plan, an internal audit of the antivirus and malware arrangements at the Council was identified to be undertaken.

## **2. Key Issues**

- 2.1 No key issues were identified in this audit. Key controls were found to be operating satisfactorily.
- 2.2 In addition, no Priority 3 recommendations were made as part of this audit.

## TERMS OF REFERENCE

### Antivirus and Malware

#### 1. INTRODUCTION

- 1.1 Antivirus software is a key component of every organisation's defence against the threats posed by malicious software ('malware' - e.g. viruses, computer worms and ransomware).
- 1.2 Antivirus software attempts to prevent the installation of known malware, as well as identifying and removing any threats identified on an organisation's computers or wider infrastructure.
- 1.3 This audit is part of the Internal Audit Plan for 2017/18 as agreed by the General Purposes and Audit Committee.

#### 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 the control environment with regards to Antivirus and Malware.
- 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 will examine the following areas associated with the system:

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Policies and Procedures	0	0	0
Antivirus and Malware Software - Technical Controls	0	0	0
User Controls	0	0	0

## DEFINITIONS FOR AUDIT OPINIONS AND RECOMMENDATIONS

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, adequacy and 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:

<b>Priority 1 (High)</b>	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
<b>Priority 2 (Medium)</b>	Control weakness that represent an exposure to risk and require timely action.
<b>Priority 3 (Low)</b>	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 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.