

Final Internal Audit Report

SQL Server Sekchek Audit

May 2018

Distribution: Executive Director Resources (Final only)
 Head of ICT & Transformation
 ICT Business Continuity & Security Officer

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

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

Executive Summary

1. Introduction.....	3
2. Key Issues.....	3

Detailed Report

3. Priority 2 Recommendation.....	4
4. Priority 3 Recommendation.....	5

Appendices

1. TERMS OF REFERENCE
2. DEFINITIONS FOR AUDIT OPINIONS AND RECOMENDATIONS..
3. STATEMENT OF RESPONSIBILITY

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 SQL Server [REDACTED] was performed based on using the Sekchek tool.
- 1.2 This SQL server is an "Extract, Transform, Load" (ETL) which is responsible for feeding Microsoft Dynamics CRM. This server is currently on premise (at Croydon) but is planned to be migrated to the "cloud" in the medium term. Capita manages the host (i.e. the hardware) and the Council's ICT function manages the application.
- 1.3 The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Issue

Four shared folders, which contain customer data from the CRM application, are accessible to everyone from the Council's network, (**Issue 1.**)

The Priority 3 issue is detailed under item 4 below.

3. Actions and Key Findings/Rationale

<u>Control Area 1: Application Management and Governance</u>	
Priority	Action Proposed by Management
2	<p>The Council has implemented this recommendation and have now restricted access to shared folders to approved users and systems only.</p>
	<p>Detailed Finding/Rationale – Issue 1</p> <p>Management should ensure that shared folders are restricted to approved users and systems.</p> <p>Four shared folders are accessible to everyone from the Council's network. These folders are namely:</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>The shared folders contain customer data from the CRM application.</p> <p>Unrestricted shared folders may expose sensitive data to all users on the Council's network, including third-parties such as Capita who have access to the network.</p>
Responsible officer	Deadline
ICT Business Continuity & Security Officer	Completed

4. Priority 3 Issue

Action Proposed by Management	Detailed Finding / Rationale
<p>1. It is neither Capita nor LBC policy to audit to this level. Therefore, we will not be implementing this recommendation.</p>	<p>The audit policy settings have default values (non-audited) and are not aligned with Microsoft recommendations. While key settings such as user logon/logoff are audited, additional events which would provide useful details for an investigation are not audited.</p> <p>Examples of non-audited events are "Process creation" or "Security System Extension", upon which modifications should be audited.</p> <p>Auditing "Process Creation" determines whether the operating system generates audit events when a process is created, which facilitates the investigations in the case of compromise.</p> <p>Auditing "Security System Extension" provides information about attempts to install or load security system extensions or services (which are critical system events) that could indicate a security breach.</p> <p>Without such information, the depth of an investigation would be limited or insufficient.</p>

TERMS OF REFERENCE

SQL Server Sekchek 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 SQL Server Sekchek will be performed.
- 1.2 The scope of this audit will look at the configuration of the security policies in the SQL Server with the aid of the Sekchek security analysis tool.
- 1.3 This audit is part of the agreed Internal Audit Plan for 2017/18.

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.

3. SCOPE





- 3.1 This audit will examine the following areas:

- System-wide Security Policies;
- Audit Policy Settings;
- Event Logs Settings;
- Registry Key Security Options Settings;
- User Accounts and Passwords;
- Rights and Privileges;
- Trusts and Remote Access;
- Services and Drivers;
- Logical Drives and Network Shares;
- Updates and Patches;
- Discretionary Access Controls; and
- Default Accounts,

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.