Final Internal Audit Report

Capita Event Management Audit

January 2019

Distribution:

Executive Director of Resources (Final only)
Chief Digital Officer
Head of Digital Services
ICT Sourcing Relationship Manager
ICT Services & Contracts Manager

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

Confidentiality and Disclosure Clause

This report ("Report") was prepared by Mazars LLP 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 LLP 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

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 The Council's IT infrastructure monitoring, software and IT assets are managed by the service provider (Capita) as part of the IT service management agreement. As part of this year's plan, an audit of Capita Events Management was performed to ensure that controls have been adequately designed and implemented to ensure effective IT Infrastructure security, capacity management and IT Software asset management.

1.2 The overall objective of this audit was to provide an objective independent opinion on the adequacy and effectiveness of the control environment with regards to IT infrastructure monitoring, software and IT assets management (Capita Event Management).

1.3 This audit was undertaken as part of the agreed Internal Audit Plan for 2018/19.

2. Key Issues

Priority 2 Issues
A large number of users (74), have access to make changes to the Remedy IT Asset Register, which contain laptops, workstations and servers & network devices. Evidence was not provided to verify if all users are authorised and need access to amend the Register, **(Issue 1).**
It was identified that the Council does not have a single IT Asset Register linking IT Assets to staff. The Council is currently utilising multiple IT Asset Registers for different assets, such as the Remedy IT Asset (for laptops, workstations, servers & network devices) and the SharePoint register (for mobile phones and tablets), **(Issue 2).**
It was identified that the process of recovering IT Assets from leavers is not operating effectively, as Asset Management does not receive notification of leavers. Furthermore, the responsibility of recovering IT Assets from leavers rests with the line managers and the departments, instead of HR and Asset Management. Therefore some assets may not be recovered from leavers, **(Issue 3).**

No Priority 3 issues were identified.

3. Actions and Key Findings/Rationale

<table>
<tr><th colspan="4"><u>Access to the IT Asset Register (Remedy System)</u></th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 1</th></tr>
<tr><td>2</td><td colspan="2">Capita's Remedy platform has in excess of 4,000 Capita staff who use the system. The support team managing the Remedy platform and the asset managers across the business make up this number. Levels of access differ across support towers meaning that not every one of the 74 users have the ability to amend every field in the CMDB. For instance, for a CI containing configuration information (disk size, network adapters etc.), the members of the relevant support team are responsible for amending detailed technical data but cannot for instance delete a complete CI.
A review of Capita users accessing the CMDB has been completed</td><td rowspan="3">Only authorised users should have access to make changes to the Remedy IT Asset Register. This review should be formalised and be performed at least once a year.
A large number of users (74), have access to make changes to the Remedy IT Asset Register, which contain laptops, workstations and servers &amp; network devices. Evidence was not provided to verify if all users are authorised and need access to amend the Register.
Unauthorised users may have access to make changes to the IT Asset Register, which may result in unauthorised amendments or deletion of assets.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Capita</td><td>Completed</td></tr>
</table>

<table>
<tr><th colspan="3">Utilisation of Multiple IT Asset Registers</th></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 2</th></tr>
<tr><td>2</td><td colspan="2">A single Asset register will be implemented by June 2019, as we migrate all our suppliers to Service Now. Service Now is a council owned ITSM tool which all suppliers will have access to and expected to maintain the asset register.</td><td rowspan="3">A single IT Asset register for all IT assets, which is kept up to date with IT assets, such as laptops and mobile phones linked to staff, enables these IT assets to be properly managed and missing assets to be identified.
It was identified that the Council does not have a single IT Asset Register linking IT Assets to staff. The Council is currently utilising multiple IT Asset Registers for different assets, such as the Remedy IT Asset (for laptops, workstations, servers & network devices) and the SharePoint register (for mobile phones and tablets).
The use of multiple IT Asset Registers may lead to difficulties in identifying and reconciling IT assets. Furthermore, it will be difficult to link IT assets to staff and to account for lost or stolen assets.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">ICT ITSM Tooling Manager</td><td>June 2019</td></tr>
</table>

<table>
<tr><td colspan="4"><b><u>Recovery of IT Assets from Leavers.</u></b></td></tr>
<tr><th>Priority</th><th colspan="2">Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 3</th></tr>
<tr><td>2</td><td colspan="2">The new HR/Recruitment platform My Resources will be delivered around April/May of 2019. This will provide a data feed into the ICT's new ITSM tool which will trigger a leaver's process for perm staff. The council has decided to not include Temp staff in My Resources and therefore this will remain as a manual process, which will trigger a leaver's form in Service Now.
This will allow for the Service Desk to recover assets properly and update the asset register.</td><td rowspan="3">An appropriate leavers process helps ensure that IT assets are returned prior to employees leaving and that IT access is disabled in a timely manner.
It was identified that the process of recovering IT Assets from leavers is not operating effectively, as Asset Management does not receive notification of leavers. Furthermore, the responsibility of recovering IT Assets from leavers rests with the line managers and the departments, instead of HR and Asset Management. Therefore some assets are not recovered from leavers.
IT Assets may not be recovered from leavers or may be reallocated to other staff members without the knowledge of the Asset Management team. This may result in inaccurate records, financial losses where assets are not recovered and possible exposure of data for unrecovered IT Assets.</td></tr>
<tr><th colspan="2">Responsible officer</th><th>Deadline</th></tr>
<tr><td colspan="2">ICT Services &amp; Contracts Manager</td><td>In progress</td></tr>
</table>

Appendix 1

TERMS OF REFERENCE

Capita Event Management Audit

1. INTRODUCTION AND BACKGROUND

1.1 The Council's IT Infrastructure Monitoring and Software Asset is managed by the service provider (Capita). As part of this year's plan an audit of the IT Infrastructure Monitoring and Software Asset Management will be performed to ensure that controls have been adequately designed and implemented to ensure effective IT Infrastructure security, capacity management and IT Software asset management.

1.2 This audit is part of the Internal Audit Plan for 2018/19 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 IT Infrastructure Monitoring and Software Asset Management.

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 The audit will included the following specific areas:

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Apply monitoring and Infrastructure events and to take action	0	0	0
The administration of the CMDB/Asset Management	0	2	0
The management of a single people record (linked to assets deployed)	0	1	0
Software and license management	0	0	0

3.2

Appendix 2

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, 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 LLP 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.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom.
Registered in England and Wales No 0C308299.