CROYDON

Final Internal Audit Report

IT Asset Management Audit

May 2023

Distribution: Interim Assistant Chief Executive
Interim Chief Digital Officer and Director of Resident Access
Business Operations Manager
Corporate Director of Resources and S151 Officer
Director of Finance (Deputy S151)

Assurance Level	Issues Identified	
Substantial Assurance	**Priority 1**	**0**
	Priority 2	**1**
	Priority 3	**1**

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.

mazars

Contents

Page

Executive Summary

Detailed Report

Appendices

1 Introduction

1.1 IT asset management (information technology asset management, or ITAM) is a set of business practices that combines financial, inventory and contractual functions to optimize spending and support lifecycle management and strategic decision-making within the IT environment.

1.2 IT Asset management is important because it helps organisations monitor and manage their IT assets using a systemised approach. Managed effectively, the benefits include improvements to productivity and efficiency which places an organisation in a better position to increase their return on investment.

1.3 Within the London Borough of Croydon (Council), whilst the responsibility for IT Asset management lies with the Corporate Technology team, this is outsourced to a third-party supplier, LittleFish, who are responsible for IT Asset Management activities such as maintaining the asset register and assigning devices to new staff members.

1.4 While our review and testing were performed remotely, we have been able to obtain all relevant documents required to complete the review.

1.5 This audit originally formed part of the agreed Internal Audit Plan for 2021/22 and is being reported now due to delays in the initiation of the audit with the Council's Corporate Technology team. The objectives, approach and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

2.1 There were no priority 1 issues arising, although one priority 2 issue has been identified:

Priority 2 Issues
IT asset management and other ITIL policies (change management, configuration management, incident management, knowledge & problem management and service request) were in a draft version, and had not been updated since May 2019. There were also examples of policies which had passed the proposed review date and not been updated. **(Issue 1)**

Details on the Priority 3 finding are included in Section 4 below.

3. Actions and Key Findings/Rationale

Control Area: Policies and Procedures

Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 1
2	All policies linked to asset management will be reviewed as part of the End User Device Project as there will be an impact on the acceptable usage policy and asset management will be more robust.	**Expected Control** Policies and procedures should be documented, up to date and version controlled. **Finding/issue** IT asset management and other ITIL policies (change management, configuration management, incident management, knowledge & problem management and service request) were in a draft version, and had not been updated since May 2019. It was also noted that the disposal document had not been formally approved, and did not have a suitable revision history. In addition, three further policies i.e. CDS computer systems and equipment use policy, CDS communication and mobile device policy, CDS laptop and tablet security policy expired in November 2021 and had not been updated. **Risk** Policy and procedure documents not being sufficiently embedded, updated or approved by management may result in staff following incorrect practices and not having a standardised process throughout the Council.
Responsible Officer	Deadline	
Business Operations Manager	End of FY 23/24	

4. Priority 3 Issue

Agreed action	Findings
Control Area: Asset Loss Management **Action proposed by management:** Asset management is within the scope of the End User Device Project and will be improved to mitigate this risk. **Deadline:** End of FY 23/24	**Expected Control** Devices that are lost/stolen should be tracked and monitored through the IT Asset Register. Updates should be made in an accurate and timely manner. **Issue/Finding** The Councils IT Service Management tool ServiceNow comprises modules for incident management, change management and asset management, amongst others. We noted that the ServiceNow asset register was not updated to reflect the status of devices when these were lost/stolen even though the loss or theft was already being monitored and managed through ServiceNow incident tickets. We noted that assets, despite being lost / stolen, ware marked as 'In use' in the asset register. There was no mechanism to update the asset register when devices were lost/stolen or to verify that all tickets for lost/stolen devices had led to the asset register entries for relevant devices being updated. However, it should be noted that in the subsequent monthly dashboards (May, June, and July 2022), this mistake had been identified and rectified. **Risk** An inaccurate asset register can lead to miscalculation and inconsistency of the council assets and create a risk in the process to manage assets.

Appendix 1

AUDIT TERMS OF REFERENCE
IT Asset Management – 2021/22

1 INTRODUCTION

1.1 IT asset management (information technology asset management, or ITAM) is a set of business practices that combines financial, inventory and contractual functions to optimize spending and support lifecycle management and strategic decision-making within the IT environment.

1.2 IT Asset management is important because it helps a company monitor and manage their IT assets using a systemised approach. Managed effectively, the benefits include improvements to productivity and efficiency which places a business in a better position to increase their return on investment.

1.3 This audit is being undertaken as part of the agreed Internal Audit Plan for 2021/22

2 OBJECTIVES AND METHOD

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.

2.2 The audit will for each controls / process being considered:

- Walkthrough the processes to consider the key controls;
- Conduct sample testing of the identified key controls, and
- Report on these accordingly.

3 SCOPE

3.1 The audit examined the Council’s arrangements for IT Asset Management.

Audit Area	Identified Issues		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Policies and Procedures	0	1	0
Asset Loss Management	0	0	0
Maintenance of the Asset Register	0	0	0
Security of Hardware	0	0	0
Assignment of Assets	0	0	0
Asset Loss Management	0	0	0
Disposal Procedures	0	0	1
Totals	**0**	**1**	**1**

Appendix 2

Definitions for Audit Opinions and Identified Issues

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 constantly 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 of the controls which may put this achievement at risk.
🟠	Limited Assurance	There are significant weaknesses in key areas of system controls and non-compliance that puts achieving the system objectives at risk,
🔴	No Assurance	Controls are non-existent or extremely weak, leaving the system open to the high risk of error, abuse and reputational damage.

Priorities assigned to recommendations are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require immediate attention by management to action and mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that still represent an exposure to risk and need to be addressed within a reasonable period.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, still provides an opportunity for improvement. May also apply to areas considered to be of best practice that can improve for example the value for money of the review area.

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: 30 Old Bailey, London EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.