

# Final Internal Audit Report

## Microsoft Azure Cloud Usage

### December 2023

Distribution: Interim Assistant Chief Executive  
Interim Chief Digital Officer & Director of Resident Access  
Head of Digital Operations  
Technology and Architecture Manager  
Director of Finance and Deputy S151  
Corporate Director of Resources and S151 Officer (Final only)

Assurance Level	Issues Identified	
Substantial Assurance	Priority 1	0
	Priority 2	2
	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.

**Contents**  
**Page****Executive Summary**

1. Introduction	3
2. Key Issues	4

---

**Detailed Report**

3. Actions and Key Findings/Rationale	5
4. Priority 3 issue	8

**Appendices**

1. Terms of Reference
2. Definitions for Audit Opinions and Identified Issues
3. Statement of Responsibility

## 1. Introduction

- 1.1 The London Borough of Croydon (the “Council”) has migrated IT infrastructure to Microsoft Azure (“Azure”) adopting an initial “lift and shift” approach. The lift and shift migration approach involved migrating existing applications and associated data to the cloud with minimal or no changes. Applications were effectively ‘lifted’ from the existing environments and ‘shifted’ as-is to a new hosting premises i.e. in the cloud. There were tools and functionality that the Council may not be using but were available to better maximise and optimise the usage of the service provided by Azure. Therefore, a review of the usage of Azure Cloud Services was performed to help ensure usage is optimised and reduce unnecessary cost.
- 1.2 Furthermore, the Council’s main IT contract with Capita ended on 31 May 2023, and hence the Council had recently established relationships with new service providers including Version One, who support all servers and Adept, who support the network.
- 1.3 With regard to two of the three scope areas, the following areas of good practice were noted:
- **Azure Landing Zone architecture** - The review found the Azure platform appeared to be well architected in line with Microsoft’s Well Architected framework; the high level and low-level architecture documents reviewed supported this; and
  - **Azure services currently being used and total cost breakup** - A set of practices was in place to monitor and review costs regularly. A Microsoft Excel based reporting process was in place, which was developed and maintained by dedicated personnel. This meant the Council was proactively reviewing and managing Azure costs. Furthermore, any new services or workloads that go into the Azure environment were reviewed and approved by the Council’s Chief Architect.
- 1.4 Overall, IT at the Council was on an improvement journey where resolution of the findings, which are inter-related, will help to support this journey from the Microsoft Azure perspective.
- 1.5 A scope limitation was agreed with regards to scope area three ‘Review the services of the top three applications that contribute the most cost’. This was because core business critical Council applications were not hosted on the Azure platform. Additionally, the top three applications that contributed the most cost could not be determined based on the billing information received. Therefore, it was agreed that this item be removed from scope with reliance being placed on scope area two above ensuring costs were being effectively monitored and managed.
- 1.6 Although out of scope of this audit, our review identified the existence of an IT Disaster Recovery (ITDR) solution based in Microsoft’s UK West region (in Wales). Primary Council services were provided from the UK South region in London. The Council may wish to consider a review of their ITDR solution in

due course to ensure it is operating effectively and services can be recovered in line with business need.

- 1.7 During the audit, Microsoft coincidentally performed an assessment of the Azure Landing zone. It was considered prudent to review this report as part of our review and commonality was found with the audit's findings. The Council is recommended to implement the recommendations made by Microsoft.
- 1.8 Whilst the review and testing were performed remotely, Internal Audit have been able to obtain all relevant documents required to complete the review.
- 1.9 This audit was undertaken as part of the agreed Internal Audit Plan for 2022/23. The objectives, approach and scope are contained in the Audit Terms of Reference at Appendix 1.

## 2. Key Issues

### Priority 2 Issues

The Azure landing zone and architecture documentation was not up to date and remained in Capita branding. A recent significant technical change had also not been reflected in the technical documentation. IT outages caused by reliance on out-dated technical documentation could result in an impact to front line Council services and / or reputational damage to the Council. **(Issue 1)**

Separate from the usual IT Administration accounts for the day to day managing of Azure services, there was only a single emergency access 'break glass' account. Should this account be required and found to be compromised, there would be no other means of gaining access to the Azure platform without Microsoft's intervention. This could result in significant delays in recovering the Council's Azure platform resulting in extended IT outages potentially impacting front line Council services and / or reputational damage to Croydon. **(Issue 2)**

One 'Priority 3' issue is included under Section 4 below.

### 3. Actions and Key Findings/Rationale

#### Control Area 1: Azure Landing Zone architecture

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 1				
2	This document will be updated as part of the Network Refresh work as this will be reviewing and potentially changing the VPN design. Changes to configurations would be based upon the implementation.	<p><b>Expected Control</b></p> <p>Correctly branded and up to date Microsoft Azure (Azure) technical documentation is in place, with amendments being made to reflect any ongoing changes.</p> <p>Up to date and accurate technical documentation is a key aspect of managing an enterprise platform as critical as Azure. Such documents help IT resources responsible to support Azure platform with reliable information thus enabling them to make changes and enhancements confidently.</p> <p><b>Finding/Issue</b></p> <p>The Council changed IT service provider from Capita to Version 1 on 31 May 2023. The High level (Azure architecture) design (HLD) and Low-level design (LLD) documents have remained in Capita branding, have not been reviewed for accuracy and do not reflect all subsequent technical changes since these were first introduced. For example, ExpressRoute (an IT service that enables the creation of private network connections between Azure data centres and infrastructure that is on Council premises, such as an office building) had been replaced with VPN (Virtual Private Network); however, the technical documentation has not been updated to reflect this significant change.</p> <p><b>Risk</b></p> <p>There are both business disruption and reputational damage risks caused by IT outages / unavailability as a result of an incorrect IT change or misconfiguration being made using outdated IT documentation. This could result in an impact to front line Council services and / or reputational damage to the Council.</p>				
	<table border="1"> <thead> <tr> <th>Responsible Officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>Head of Corporate Technology</td> <td>30 April 2024</td> </tr> </tbody> </table>	Responsible Officer	Deadline	Head of Corporate Technology	30 April 2024	
Responsible Officer	Deadline					
Head of Corporate Technology	30 April 2024					

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 2
2	Additional emergency access account will be added.	<p><b>Expected Control</b></p> <p>Emergency access accounts are highly privileged, and these are not assigned to specific individuals. Emergency access accounts are limited to emergency or 'break glass' scenarios where normal IT administrative accounts is unavailable or compromised.</p> <p>Two emergency access accounts is recognised as good practice and provides resilience. Given the nature of these accounts (and the damage that could be done with these in the wrong hands), too many accounts then becomes a security risk in itself.</p> <p><b>Finding/Issue</b></p> <p>There were a number of key tactical recommendations provided by Microsoft during their recent assessment of the Council's 'Azure landing zone'. Amongst those, it was highlighted that there was a pressing need to implement one of these recommendations to further secure the platform.</p> <p>The Council's Azure platform only had a single emergency access 'break glass' account, if this account had been compromised, there would have been no other means of gaining access to the Azure platform without Microsoft's intervention.</p> <p>It was noted that the Microsoft review coincided with this internal audit review - it was therefore considered prudent to review this report as part of the audit for completeness. As it coincided with the audit, it was not a case of failure to implement recommendations from a previous report from Microsoft.</p> <p><b>Risk</b></p>

Responsible Officer	Deadline	
Head of Corporate Technology	31 December 2023	Significantly delays in recovering Azure cloud operations resulting in extended IT outages resulting in an impact to front line Council services and / or reputational damage to the Council.

#### 4. Priority 3 Issue

Agreed action	Findings
<p><b><u>Control Area 1: Azure Landing Zone architecture</u></b></p> <p><b><u>Action proposed by management:</u></b> The recommended setting will be enabled.</p> <p><b><u>Responsible Officer:</u></b> Head of Corporate Technology</p> <p><b><u>Deadline:</u></b> 31 December 2023</p>	<p><b>Expected Control</b></p> <p>‘Resource locks’ prevent the accidental or malicious deletion or modifications of critical shared IT services by people who have elevated access permissions to the IT platform.</p> <p>For example, IT set-up a VPN service and then enable either ‘Cannot Delete’ or ‘Read Only’ to protect it from unauthorised changes. The original user still has full access. As a precaution, the emergency break glass account can be used (see Issue 2 above).</p> <p><b>Finding/Issue</b></p> <p>The Council had not enabled the ‘prevent service termination’ setting (i.e., by turning on the resource locks).</p> <p><b>Risk</b></p> <p>Critical services and resources running in Azure were at risk of being accidentally deleted. Configurations and data could have been deleted resulting in the need to either restore from back-up or be fully rebuilt.</p> <p>Accidental deletion of shared services may have caused business disruption by making IT services unavailable or inaccessible. This could have been for a significant period of time based on the nature of the issue and result in an impact to front line Council services and or reputational damage for the Council.</p>



## AUDIT TERMS OF REFERENCE

### Microsoft Azure Usage

#### **1. INTRODUCTION**

- 1.1 There are few organisations that do not rely on third parties to support the delivery of IT services. Whilst most organisations now follow a cloud first strategy, others outsource the provision of IT services to third parties. Typical drivers for this can be cost reduction, skills deficiency, or the provision of specialist services.
- 1.2 The Council has migrated IT infrastructure to Microsoft Azure (“Azure”) adopting a “lift and shift” approach. There are tools and functionality that the Council may not be using but is available to maximise and optimise the usage of the service provided by Azure. Therefore, a review of the usage of Azure Cloud Services would be beneficial to provide assurance on what is used but also to provide recommendations on how to maximise their usage.
- 1.3 The Council has an internal IT / Digital team but continues to be reliant on third party IT service providers.
- 1.4 This audit was undertaken as part of the agreed Internal Audit Plan for 2022/23.

#### **2. OBJECTIVES AND METHOD**

- 2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of the design and operating effectiveness of controls / processes with regard to Microsoft Azure cloud usage at the Council.
- 2.2 The audit will for each control / process being considered:
  - Review the architecture documents such as Design specification;
  - Review Azure costs with breakup of cost by services;
  - Conduct interviews with key IT personnel (Architects/developers/administrators); and
  - Report on the findings accordingly.

**3. SCOPE**

3.1 This audit, focused on Microsoft Azure usage, was undertaken as part of the 2022/23 Internal Audit Plan. The specific scope included the following areas and issues identified:

Audit Area	Identified Issues		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Azure Landing Zone Architecture	0	2	1
Azure services currently being used and total cost breakup	0	0	0
Review the services of the top three applications that contribute the most cost	0	0	0
<b>Totals</b>	<b>0</b>	<b>2</b>	<b>1</b>

3.2 The audit involved a high level review of each of the below areas:

- Azure Landing Zone architecture including network, security and resiliency;
- Azure services currently being used and total cost breakup by each service per month for past 12 months; and
- Review the services of the top three applications that contribute the most cost.

3.3 The audit examined the Council’s Azure services being used, with a focus in the following areas:





- Usage - establish the services currently in use;
- Cost - establish the current cost against each of the service families; and
- Optimal Usage - establish the optimisation opportunity (if any) for top 3 applications in terms of service usage and cost.

The scope of work above was aligned to industry standards / good practice, including for example, Azure Well Architected Framework.

**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 identified issues are based on the following criteria:

<b>Priority 1 (High)</b>	Fundamental control weaknesses that require immediate attention by management to action and mitigate significant exposure to risk.
<b>Priority 2 (Medium)</b>	Control weakness that still represent an exposure to risk and need to be addressed within a reasonable period.
<b>Priority 3 (Low)</b>	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.