

# Final Internal Audit Report

## MyAccount & MyApp Application Audits

### September 2018

**Distribution:**

- Executive Director Resources (Final only)
- Head of ICT & Transformation
- Information Manager
- ICT Service & Contract Manager

Assurance Level	Recommendations Made	
<b>Limited Assurance</b>	Priority 1	1
	Priority 2	3
	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

## Contents

Page

### Executive Summary

3. Actions and Key Findings/Rationale .....	4
4. Priority 3 Issue.....	8

### Appendices

1. My Account Application - Terms Of Reference
2. My App Application - Terms Of Reference
3. Definitions For Audit Opinions And Recommendations
4. Statement Of Responsibility

**Executive Summary**

**1. Introduction**

- 1.1 The MyAccount application is used as a tool for citizens to access council services faster. Some of these services include council tax, business rates and benefits claims. The application allows citizens to check their current balance, payments and instalments due online 24 hours a day 7 days a week.
- 1.2 The MyApp application is used as a tool for citizens to report a number of issues directly to the council through the use of a mobile application. Some of the issues which can be reported via this medium include abandoned vehicles, blocked drains and gullies, empty properties, graffiti, illegal campsites, illegal street trading, pavement defects, potholes and road defects.
- 1.3 The applications were historically hosted offsite by a third party service provider but have recently been migrated into the Croydon data centre at the Council. These audits were part of the Internal Audit Plan for 2017/18. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.
- 1.4 Subsequent to the internal audit being completed, MyApp was replaced in June/July 2018, but the MyAccount remained unchanged.

**2. Key Issues**

Priority 1 Issues
No formal change management process was in place to track changes which impact the applications, <b>(Issue 1.)</b>
Priority 2 Issues
System Management responsibilities were not formally defined, <b>(Issue 2.)</b>
No user access reviews were taking place and the module for tracking system activity had not been enabled, <b>(Issue 3.)</b>
There had not been a disaster recovery test, <b>(Issue 4.)</b>

The Priority 3 recommendation is detailed under item 3 below.

3. Actions and Key Findings/Rationale

<b>Control Area 6: Change Controls</b>						
<b>Priority</b>	<b>Action Proposed by Management</b>	<b>Detailed Finding/Rationale – Issue 1</b>				
1	<p>Croydon Council is reviewing the change management process both from the point of view of initiating requests and the associated release management (deploying the changes to production environments). This will address this matter for MyAccount and the app. In the interim the CRM team will implement such a process restricted to the area covered by the application collection: MyAccount; "the app" (now called DMWC); and the CRM environments (online, VMWare servers and Azure components).</p>	<p>There is currently no formalised procedure which covers the change management process for the MyAccount and MyApp applications. In order to ensure a consolidated and standardised understanding and compliance with the process, as well as to encourage effective staff commitment and responsibility, the change management process should be documented, implemented and operated for the application. The procedure/policy should clearly describe how change requests are initiated/logged, impacted, processed, tested, approved and deployed and should be formally approved by management, acknowledged by all relevant staff and periodically reviewed.</p> <p>Without such a change management procedure and controls supporting the operation of the procedure, the Council may not be able to adequately maintain, update and change the application appropriately.</p>				
	<table border="1"> <thead> <tr> <th><b>Responsible officer</b></th> <th><b>Deadline</b></th> </tr> </thead> <tbody> <tr> <td>CRM Manager</td> <td>December 2018</td> </tr> </tbody> </table>	<b>Responsible officer</b>	<b>Deadline</b>	CRM Manager	December 2018	
<b>Responsible officer</b>	<b>Deadline</b>					
CRM Manager	December 2018					

<b><u>Control Area 1: Application Management and Governance</u></b>					
<b>Priority</b>	<b>Action Proposed by Management</b>				
<b>2</b>	The roles and responsibilities will be documented.				
	<table border="1"> <thead> <tr> <th><b>Responsible officer</b></th> <th><b>Deadline</b></th> </tr> </thead> <tbody> <tr> <td>CRM Manager</td> <td>September 2018</td> </tr> </tbody> </table>	<b>Responsible officer</b>	<b>Deadline</b>	CRM Manager	September 2018
<b>Responsible officer</b>	<b>Deadline</b>				
CRM Manager	September 2018				
	<p><b>Detailed Finding/Rationale – Issue 2</b></p> <p>It is expected that system management responsibilities are clearly defined for the ICT team and that appropriate application governance is in place to ensure that key system management requirements are identified and implemented.</p> <p>Enquiry of the CRM Manager noted that system management responsibilities were not formally defined. Day to day responsibilities for the MyAccount application were in place as this was managed by the CRM Manager. However, users within the ICT team did not have defined roles which cover the system management of the MyAccount application.</p>				

<b><u>Control Area 2: System Security</u></b>	
<b>Priority</b>	<b>Action Proposed by Management</b>
2	<p>Events were being logged, but the Microsoft module to use those data was inflexible (this was the auditing module being evaluated). Microsoft have now made the reporting more configurable so we now have the ability to report on events of our choosing.</p> <p>The Application Architects control access to this and as it is now in place, this action can be regarded as complete already.</p>
	<b>Detailed Finding/Rationale – Issue 3</b>
	<p>It is expected that appropriate audit trail functionality is in place and enabled to identify changes that have been made on the application. The changes should record user ID, date and time as well as the event taking place in addition to the activity/transaction type.</p> <p>Enquiry of management noted that within the MyAccount application there is a module which can be enabled in order to track system activity. However, Croydon has not currently enabled this feature although we acknowledge that there is an ongoing exercise being undertaken to test the audit trail feature. The team did not have defined roles which cover the system management of the MyAccount application.</p>
<b>Responsible officer</b>	<b>Deadline</b>
N/a	Implemented

**Control Area 7: System Resilience and Recovery**

<b>Priority</b>	<b>Action Proposed by Management</b>	<b>Detailed Finding/Rationale – Issue 4</b>
2	<p>This is not a matter for just one application area. If our Azure environment were to fail, or CRM online, we would be dependent upon Microsoft and the overall support that is included in the move to cloud computing.</p>	<p>In order to help confirm that the system back-ups work as required and that the system can be recovered in a timely manner in the event of a disaster, appropriate disaster recovery testing, to address the recovery from a disruption and to support business continuity arrangements for the MyAccount and MyApp application, should be put in place.</p> <p>We noted from enquiry that no disaster recovery testing has taken place in relation to the MyAccount and MyApp applications.</p>
<b>Responsible officer</b>	CRM Manager	
<b>Deadline</b>	September 2018	

4. Priority 3 Issue

Action Proposed by Management	Findings
<p>We will conduct periodic reviews of CRM (I assume that where it mentions MyAccount it means CRM, because employees don't have access to MyAccount – it's the customer portal.).</p>	<p>In order to ensure access is appropriately restricted, a periodic review should be conducted covering all users at both network and applications levels. The review should include, but not be limited to:</p> <ul style="list-style-type: none"> <li>- Users that have not logged on (the network/application) for more than 90 days;</li> <li>- Generic accounts;</li> <li>- Checking that segregation of duties is appropriately enforced.</li> </ul> <p>It was noted from enquiry of the CRM Manager that there were no user access reviews taking place to determine whether access was appropriately restricted for employees who use the MyAccount application.</p>



## TERMS OF REFERENCE

### My Account Application Audit

#### 1. INTRODUCTION AND BACKGROUND

- 1.1 The MyAccount application is intended to be a faster way for citizens to access their council tax account, business rates account, benefits claim or landlord payment schedules depending on their needs. The application allows citizens to check their current balance, payments made and instalments due online 24 hours a day 7 days a week.

The application was historically hosted offsite by a third party service provider but has recently been migrated into the Croydon data center at the Council.

- 1.2 This audit is part of the Internal Audit Plan for 2017/18 as agreed by the General Purposes and Audit Committee.

#### 2. PURPOSE 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 the MyAccount application.
- 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 (and control objectives) associated with the system:

##### **Application Management and Governance**

Application ownership and application management arrangements are in place, appropriately assigned and defined. The application is adequately licensed and that users are provided with sufficient training/guidance on the correct use of the Application.

##### **System Security**

Access to the application and its database is restricted and user activity can be monitored. Controls that prevent the application being hacked, compromised, rendered unavailable to be used, including controls over how citizens are authenticated with their user accounts are in place and effective.

##### **Interface Controls and Processing**

Data processed by the application is accurate, complete and that there are adequate reconciliation procedures in place.

**Data Input**

Information input on to the application is accurate, complete and that the application is configured to report on erroneous data prior to processing.

**Data Output**

Output reports generated by the application are adequate and that output generation is controlled.

**Change Controls**

Changes to the application follows an established procedure and any changes are reviewed and tested before being applied to the application's live environment.

**System Resilience and Recovery**

Backup and recovery arrangements for the application are in place and performed in alignment to the Business Continuity plans of the Council.

**Support Arrangements**

Arrangements are in place with the application's supplier, which is monitored on a routine basis.

## TERMS OF REFERENCE

### My App Application Audit

#### 1. INTRODUCTION AND BACKGROUND

- 1.3 The My Croydon app is a faster way for citizens to report issues to the Council using their smartphones. Using the app, citizens can report a number of issues directly into the council's computerised systems, helping to speed up the processing time for dealing with it. Issues such as; abandoned vehicle, blocked drains and gullies, empty properties, graffiti, illegal campsite, illegal street trading, pavement defects, potholes and road defects.

The application was historically hosted offsite by a third party service provider but has recently been migrated into the Croydon data center at the Council.

- 1.4 This audit is part of the Internal Audit Plan for 2017/18 as agreed by the General Purposes and Audit Committee.

#### 2. PURPOSE AND METHODOLOGY

- 2.4 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 My App application.
- 2.5 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.
- 2.6 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

- 3.2 This audit will examine the following areas (and control objectives) associated with the system:

##### **Application Management and Governance**

Application ownership and application management arrangements are in place, appropriately assigned and defined. The application is adequately licensed and that users are provided with sufficient training/guidance on the correct use of the Application.

##### **System Security**

Access to the application and its database is restricted and user activity can be monitored. Controls that prevent the application being hacked, compromised, rendered unavailable to be used, including controls over how citizens are authenticated with their user accounts are in place and effective.

##### **Interface Controls and Processing**

Data processed by the application is accurate, complete and that there are adequate reconciliation procedures in place.

**Data Input**

Information input on to the application is accurate, complete and that the application is configured to report on erroneous data prior to processing.

**Data Output**

Output reports generated by the application are adequate and that output generation is controlled.

**Change Controls**

Changes to the application follow an established procedure and any changes are reviewed and tested before being applied to the application's live environment.

**System Resilience and Recovery**

Backup and recovery arrangements for the application are in place and performed in alignment to the Business Continuity plans of the Council.





**Support Arrangements**

Arrangements are in place with the application's supplier, which is monitored on a routine basis.

## 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:

<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 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.