MAZARS

CROYDON

Final Internal Audit Report
Uniform IT Application
December 2019

Distribution:

Executive Director of Resources and Monitoring Officer (Final only)
Chief Digital Officer
Head of Digital Operations
Business Manager
Digital Business Partner

Assurance Level	Issues Identified	
Substantial	Priority 1	0
	Priority 2	3
	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 has 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 4 of this report for further information about responsibilities, limitations and confidentiality.

Contents

Page

Executive Summary

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 Uniform is a key line of business ICT system used primarily within the Place department across the following diverse service areas: planning, building control, environmental health, food safety, trading standards, commercial licensing, pollution, and residential property enforcement. This system has been used for over ten years and as part of recent governance around contract extensions, Contracts and Commissioning Board (CCB) stipulated that the system should be subject to a full market review. Therefore, a project is currently underway to prepare tender documentation for the re-procurement of the Uniform IT application.

1.2 Uniform's current deployed mobile working solution for Building Control, Kirona (hand-held mobile GPS device), requires a good mobile signal strength to operate effectively which is often not the case. Other service areas using Uniform currently have no mobile working solution. Therefore, mobile working officers have to manually upload information into the Uniform IT application, when they are next in the office, resulting in delays to updating the system and increasing the potential risk of entering data inaccurately and incompletely.

1.3 The overall Uniform IT application is administered by the Applications Team, which consists of one full time member of staff who is supported by another member of staff working part time, (approximates to 1.1 FTE). The Council out-sourced its Applications Team under a Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE agreement) with Capita. The TUPE agreement was reversed on 15 May 2019 and the Applications Team was brought back in house to continue its responsibility for administering the Uniform IT application. When the Applications Team were out-sourced to Capita, there were two full-time application support officers responsible for Uniform. One of these retired prior to the team returning to CDS, and was not replaced.

1.4 On 15 May 2019 the outsourced support model transitioned to a multi-vendor arrangement (from the single offering provided by Capita). The hosting and management of virtual servers is still outsorced to Capita, including the Citrix servers which host the Uniform system. The administrative tasks are undertaken by the Applications Team, but are not documented, increasing the risk that in their absence (e.g. holiday or sickness) no one else, including the 'super-users', has been trained on how to perform them.

1.5 The Council's new support model transition also saw its service desk function outsourced to Littlefish, who has minimal knowledge on how to use the Uniform IT application but help triage logged incidents and requests to support the infrastructure the infrastructure on which it is hosted.

2. Key Issues

Priority 2 Issues
There is reliance on two key members of staff and a lack of documented procedures, checklists/timetables to provide guidance on how, what and when administrative tasks need to take place. **(Issue 1)**.

Line managers do not provide sufficient information when asking for new starters to be set up and there were no documented procedures for notifying changes in users or for leavers. **(Issue 2)**
When the Applications Team was bought back in house during May 2019, the Council became responsible for disaster recover arrangements of the Uniform IT application; however, they are still to write, implement and test a disaster recorvery plan. **(Issue 3).**

One Priority 3 issue was also identified and is included under item 4.

3. Actions and Key Findings/Rationale

<table>
<tr><th colspan="3"><u>Control Area 01: Application Management and Governance – System administrative tasks.</u></th></tr>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale – Issue 1</th></tr>
<tr><td>2</td><td>This risk was one of the reasons why the applications team was brought back in-house as it was recognised that Capita’s contract didn’t provide full ownership in a number of areas.
Work <b>already undertaken</b> to mitigate some of the risk includes:
1. Four other members of the application team have been on Idox-run training courses so there is more awareness across the team;
2. New team manager has implemented an initiative to provide documentation for FAQs and resolution of common issues so the workload can be shared in the event of leave, etc
Both of these are the initial steps and won’t fully mitigate the risk identified.
A draft <i>systems handbook</i> has been created and will evolve over time. The priority areas to be completed will be the checklists of common tasks as highlighted here <b>(Target date 31/1/20)</b>.
The reprocurement of the current solution has a key decision point expected to be mid-Feb 20 where the procurement</td><td>The Council’s Applications Team was brought back in-house during May 2019, following a six year period of being out-sourced to Capita. Of the officers responsible for looking after the Uniform application, only 2 out of 3 members of staff that TUPED to Capita were TUPED back to the Council during this process, as one member of staff retired and has not been replaced.. The remaining staff responsible for administering the Uniform IT application (e.g. running backups, setting up new users and making configuration changes) are very experienced and knowledgeable; however, there is a key dependency on these 2 staff members. Whilst, there are super users who provide guidance on how to use the Uniform IT application, they have not been trained to run the administrative tasks.
Furthermore, there are no documented procedures, checklists/timetables to provide guidance on how, what and when administrative tasks need to take place.
As the Uniform IT application re-procurement process is underway, it is accepted that full documentation of the administrative procedures may not be apropriarte at this point in time. However, once the re-procurement process has completed the administrative procedures should be documented as a matter of priority (either for Uniform or for the application that replaces it).
In the interim, the Uniform IT application team should prepare as a minimum, a high-level checklist of tasks that need to be completed on a daily, weekly, monthly and ad-hoc basis, and train some of the super users on how to run these administrative tasks.
There is an increased risk that in the absence of these 2 key staff members (due to them being on annual or sick leave at the same time) and documented procedures, there would be no guidance or support on how to undertake the administrative tasks for the Uniform IT application.</td></tr>
</table>

	strategy will be agreed. The tender process and implementation of an alternative solution (should Uniform not be the preferred bidder) is a minimum of 18-24 months after that so it is key to ensure appropriate documentation is in place to cover the administration and support of the current system. CDS have committed to a restructure of the current applications team and the currently separate Business Systems Support team to agree common roles, responsibilities, and processes to better support our service users (start due Jan 20). Conclusion of this exercise is expected to help the balance of work and improve multi-skilling across all key applications to minimise the exposure to this risk. **(Target date 30/4/20)**.	
Responsible officer	**Deadline**	
Head of Digital Operations	30/4/20	

Control Area 02: System Security – Starters, leavers and movers in relation to the Uniform IT application.

Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 2
2	The risks identified here are not isolated to Uniform but all applications in use at Croydon. It is an issue that despite perstistent attempts to address elements of the process, finding a robust and consistent solution is hampered by the complexities of key data needed to enforce the rules being owned and managed across multiple service areas and systems. **Starters** We will undertake a review to assess the impact of not allowing mirroring as part of the account setup process. **(Target date 31/3/20)**. **Movers** We will undertake a review to determine whether developing a Service Now online request form would help service managers report changes in roles so we can then investigate whether this impacts system access requirements. **(Target date 31/3/20)**. **Leavers** We will undertake a review to determine the feasibility of freezing accounts not accessed for a period of time (6 weeks?). **(Target date 31/3/20)**.	**Starters** It was noted that starters cannot be setup on the Uniform IT application without having an Active Directory (AD) account setup first. This is triggered by an extract from the HR system being automatically sent to Littlefish for the creation of an employee ID. This is then used to create a 'skeleton' Active Directory account to provide network access. Business managers then submit a form in Service Now to create a business system account to request access for specific applications, including Uniform. Service Now then passes the request to the Applications Team to create the business system accounts. It was noted that business managers do not provide adequate information defining what access rights a new starter should be granted based on their job description, instead they ask for new starter accounts to mirror those of an existing user whose job description may differ from that of the new starter. **Movers and Leavers** There is no official process of notifying the Applications Team when a user of the Uniform IT application: • Changes role requiring their access privileges to be increased or decreased; • Leaves the Council requiring their access to be revoked. However, there are ad-hoc requests from some business teams requesting that leavers access be revoked; and • Whilst, a process is in place for revoking access to AD when someone leaves this information is not always shared with the Applications Team allowing them to disable the leaver's Uniform IT application account. There is an increased risk that users of the Uniform IT application may: • Have more access than is required for their current role; or • Not have their accounts revoked in a timely manner following their departure from the Council.

Responsible officer	Deadline
Head of Digital Operations	31/3/20

Control Area 07: System Resilience and Recovery – Disaster Recovery arrangements for the Uniform IT application.		
Priority	**Action Proposed by Management**	**Detailed Finding/Rationale – Issue 3**
2	CDS are addressing this risk on two fronts. Firstly, prior to terminating the Capita contract it became apparent that the proposed DR solution was not 100% fit for purpose so was mitigated by ensuring key system backups were saved in Croydon's Microsoft Azure Cloud environment. This would enable restoration to virtual servers that would be built in the event of a disaster scenario. With the new multi-vendor support model work needs to be undertaken to agree roles, responsibilities and supporting procedures which would kick-in once a disaster scenario occurred. **(Target date 31/3/20)**. It is proposed to accept the risk of not formally testing this plan at this stage due to the following activities. Secondly, Croydon's Cloud First architectural principle is driving a number of key projects. Core infrastructure services have already been migrated to Azure Cloud and all applications will be moved from the current data centre before May 2021. In terms of Uniform, discussions have already taken place with Idox (suppliers of Uniform) and their support of the migration of the entire Uniform server infrastructure has been discussed and quoted for.	It was noted that when the Applications Team was part of Capita, pre May 2019, Capita was responsible for disaster recovery (DR) arrangements of the Uniform IT application however, these arrangements were not tested. When the Applications Team was bought back in house during May 2019, the Council became responsible for DR arrangements of the Uniform IT application; however, they are still to write, implement and test a DR plan. Not having a DR plan in place increases the risk of: • Data loss – which can occur in a number of different ways e.g.natural disaster, security breaches and human error; • Business interruption – loss of staff productivity and the inability to service the needs of those living in the Borough; and • An expensive recovery - cost to replace hardware and rekey data.

	Due to project dependencies and lead times we expect to start the detailed planning for the migration during March 20, with the actual migration taking place between May and Aug. **(Target date 31/8/20)**. A DR test of the new solution is not expected until the programme is completed. Moving the Uniform application server into the Cloud also mitigates a separate risk of that being an ‘old’ physical server – the age arguably increasing the likelihood of a significant outage (not necessarily a disaster). Finally, as part of the re-procurement discovery work, we will be revisiting with the service what their expectations of system restoration turnaround in the event of a disaster is as it is not clear when this was last asked and we need to ensure the final solution meets user need. **(Target date 31/1/20)**.	
Responsible officer	**Deadline**	
Head of Digital Operations	31/8/20	

4. Priority 3 Issue

Action Proposed by Management	Findings
The decision to deploy Service Now as a solution owned by Croydon, rather than rely on a service partner to run the service management toolset was a key initial part of getting back control of vital information we could then use to drive service improvements based on factual evidence. There are a number of improvements in the backlog for both process and Service Now toolset which aim to make it easier for service users to report common issues. Also, part of the CDS commitment to restructure the current applications team and the currently separate Business Systems Support team will include a 'deep dive' of the type of work which commonly bypasses the official channels. The outcome of this analysis will drive: 1. Clearer roles, responsibilities and expectations as part of the revised structure; and, 2. A communications plan to appropriate stakeholders and common offenders to change behaviours to the preferred support channels.	Business users are familiar with members of the Applications Team and often approach them directly when they have an issue with the Uniform IT application. It was noted that whilst these issues are resolved, they are not always reported to Littlefish for logging into the support desk system Service Now. Not logging all Uniform IT application related issues into Service Now increases the risk that Management will not have complete visibility over the total number and types of issues being encountered, have the ability to analyse issues for recurring problems that require fixes and whether the size of their in-house Applications Team is adequate.

Appendix 1

TERMS OF REFERENCE

1. INTRODUCTION AND BACKGROUND

1.1 The Uniform IT application is a key line of business system used by the following services:

- Planning (development control and spatial planning);
- Building Control (BC);
- Commercial Licensing (e.g. permits for pubs, clubs, events, skips, scaffolding etc);
- Trading Standards;
- Food Safety (i.e. monitoring of food premises and issuing of the 5* ratings);
- Environmental Health;
- Pollution;
- Neighbourhood Safety (e.g. graffiti, abandoned cars, fly tips, etc);
- Residential housing enforcement; and
- Housing grants.

1.2 It is supplied by Idox and, although it is referred to as ‘Uniform’, it comprises a number of separate Idox systems which integrate together, specifically:

- Uniform application;
- Document Management System;
- Public Access (for applicants to comment on planning applications);
- Idox online forms (being tested);
- Idox mobile working apps (being tested); and
- Kirona mobile app (used by BC).

1.3 The Uniform application audit will be performed to ensure that controls have been adequately designed and implemented to ensure effective IT security, linkages/interfaces with other council infrastructures and systems.

1.4 This audit is part of the Internal Audit Plan for 2019/20 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 the Uniform 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 examined the following areas:

Control Areas/Risks	Issues Identified		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Application Management and Governance	0	1	0
System Security	0	1	0
Interface controls and processing	0	0	0
Data Input	0	0	0
Data Output	0	0	0
Change Control	0	0	0
System resilience and recovery	0	1	0
Support arrangements	0	0	1
TOTAL	**0**	**3**	**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 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 identified issues 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 represents an exposure to risk and requires 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.