CROYDON

Final Internal Audit Report

IT Service Provider - Capita Exit & LittleFish delivery of service

November 2024

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

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

forvis mazars

Contents

Page

Executive Summary

Detailed Report

Appendices

1. Introduction

1.1 There are few organisations that do not substantially rely on third parties to support the delivery of IT services. This has only increased since the advent of cloud computing. Many organisations now follow a cloud first strategy, which includes the outsourcing of IT services to third parties for 'Software as a Service' cloud offerings. Typical drivers for this can be cost reduction, skills deficiencies, or for the provision of specialist services.

1.2 The London Borough of Croydon (the Council) contracted with Capita in 2013 for it to host and manage a range of IT services over a nine-year term at an expected cost of £63m across the period. In 2018, an internal audit report concluded a review of the management of the contract and noted underperformance by Capita against the contractual service levels and Key Performance Indicators (KPIs). For this reason, we were informed by the Head of Corporate Technology, that a series of Change Control Notices (CCNs) had been used to gradually novate some services to be delivered by other service providers. Although the original contract expired in May 2022, it was extended for a further 12 months to allow for novation of the remaining services to take place.

1.3 Known as the Capita Exit project, this was supported by an exit plan with a timeline, an outline structure with roles set out, and a scope for the project with defined goals. Furthermore, controls were put in place to mitigate risks associated with the project, such as project monitoring, risks & issues management, and change controls.

1.4 Beyond Capita, the Council also outsources its IT service desk and related service support activities to Littlefish with whom IT management advised, at the time of review, provided a satisfactory service.

1.5 One of the scope areas included in this internal audit is "Littlefish Risks and Controls". For this scope area, we selected a sample of four services for review; Service Request Management, Incident Management, Problem Management and Change Management. Each process, whilst lacking recent approval is documented with step-by-step processes and roles and responsibilities, that are based on the good practice IT Infrastructure Library (ITIL) guidance. Other internal audits recently conducted covering Cyber Security and IT Asset Management provide further assurance for additional services provided by Littlefish that were not tested in this internal audit.

1.6 Incidents reported to the Littlefish service desk are resolved with reference to a knowledge management database and tracked against KPIs for 'First Time Fulfilment'. The monthly Service Review reports from Littlefish, between March 2022 and December 2022, report that the IT service desk achieved a 'First Time Fix' rate of 99%.

1.7 Problems which are defined 'as the unknown underlying root cause of one or more incidents or a condition identified as the cause of multiple incidents that exhibit similar symptoms' are classified according to their priority with their

impact and urgency recorded. Additionally, Littlefish provides weekly problem review reports to the Croydon IT Operations team showing trends and detailed updates on open and closed problems.

1.8 The IT Change Management process governs all changes to production systems. Depending on the type of the change, the process includes a set of controls, such as documenting a backout plan, carrying out a risk and impact analysis, pre-production testing, and a post implementation review. Additionally, a weekly Change Advisory Board (CAB) assesses the changes for approval.

1.9 Required service levels and KPIs are defined for the IT services provided by Littlefish, and monthly reports are submitted to the Council for it to track and evaluate the effectiveness of the service provided.

1.10 Whilst this was completed audit remotely, we have been able to obtain all relevant documentation and review evidence via screen sharing functionality to enable us to complete the work. This audit was undertaken as part of the agreed Internal Audit Plan for 2021/22. However, due to delays in the delivery of other IT audits, this audit was not undertaken until the 2022/23 period.

2. Key Issues

Priority 3 issues are raised in Section 3 below.

3. Priority 3 Findings

Agreed action	Findings
Control Area 1: Reporting and Governance **Action proposed by management:** The End User Services provision is being reviewed at present to procure and reform from March 2025. As part of this work the process documents will be reviewed to meet the changes to the model. I will ensure that a review of all documents is conducted in the short term to ensure that they are fit for purpose and reflect the current processes. **Responsible Officer:** Business Operations Manager **Deadline:** January 2025	**Expected Control** Processes should be documented and help govern the effective delivery of IT Services. The documented processes should be reviewed and updated on a regular basis and whenever major organisational changes take place. Version control should also be incorporated. **Issue/Finding** Several processes relevant to the internal audit were confirmed to be documented with step-by-step guidance and with roles and responsibilities outlined. However, process documents listed below for key processes were recorded as last reviewed on the 15th of May 2019, and some of these did not reflect the current practices in place. For example, it was noted in the IT Change Management process document, that the Change Advisory Board (CAB) meets twice a week, whilst the CAB actually meets once a week. Additionally, the listed process documents did not include a next review date or a review cycle. The process documents reviewed were: - Change Management Process, - Incident Management Process, - Problem management Process, - Service Request Process, and - Knowledge Management Process. **Risk** The lack of reviews and updates for process documents may result in them becoming outdated so that they are no longer aligned with the evolving business

Agreed action	Findings
	environment and may not reflect the current best practices or incorporate the necessary updates. This could cause potential non-compliance with requirements, leading to potential delays, issues and ineffective IT service delivery.
Control Area 5: Littlefish Risks and Controls - Change Management **Action proposed by management:** Since this change was implemented, we have reviewed our Change Process and now do not accept any changes, be it normal, standard, or emergency change unless all fields are populated with the relevant information required. Simply putting N/A is not acceptable. All changes that come to CAB must be fully documented to explain what the change is, impact, risk, testing, backout plan etc. We are very strict on this. As the council's IT Service Delivery Manager who is responsible for the Change Advisory Board, I am satisfied that this audit finding is resolved. **Responsible Officer:** Business Operations Manager / Digital Service Delivery Manager **Deadline:** Complete	**Expected Control** The IT Change Management process should be documented, and the process developed should be adhered to where appropriate testing is carried out with formal approval for delivery. **Issue/Finding** From the review of a sample of six IT changes, it was noted that one Emergency change (CHG0032438) did not follow the process developed, where a backout plan was not recorded, and the risk and impact analysis as well as pre-production testing and the Post Implementation Review were not carried out. **Risk** Not adhering to the IT Change Management process may increase the risk of system failures and service disruptions as the change is not correctly delivered first time. It also risks the ability to effectively respond to issues, recover from failures and maintain the reliability of the IT environment.

Appendix 1

AUDIT TERMS OF REFERENCE

IT Service Providers

1. INTRODUCTION

1.1 There are only a few organisations that do not substantially rely on third parties to support the delivery of IT services. This has only increased since the advent of cloud computing. Most organisations now follow a cloud first strategy, which includes the outsourcing of IT services to third parties for 'Software as a Service' cloud offering. Typical drivers for this can be cost reduction, skills deficiency, or for the provision of specialist services.

1.2 The Council has an internal IT/Digital team but continues to be reliant on third party IT service providers.

1.3 The Council contracted with Capita in 2013 for it to host and manage a range of IT services over a nine-year term at a cost of £73m. Subsequently, in 2018, an internal audit report concluded a review of the management of the contract and noted underperformance by Capita against the contractual service levels and Key Performance Indicators (KPIs). For this reason, we were informed by the Head of Corporate Technology that a series of Change Control Notices (CCNs) have been used to gradually novate the contract for some services to be delivered by other service providers. Although the original contract expired in May 2022, it was renewed for 12 months to allow for the novation of the remaining services to take place.

1.4 Beyond Capita, the Council also outsources its IT service desk and related service support activities to Littlefish with whom IT management considers the current service to be satisfactory.

1.5 The 2018 audit of the Council's management of the Capita contract gave an assurance rating of Limited. There have been no further audits on IT service provision though other audits such as those on cyber security and asset management may have assessed controls that are operated by third parties where relevant.

1.6 This audit is being undertaken as part of the agreed Internal Audit Plan for 2021/22. However, due to delays in the delivery of other IT audits, this audit has been moved to the 2022/23 period.

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 involve the following for each controls/process being considered:

- Walkthrough of the processes to identify the key controls;
- Sample testing of the identified key controls; and
- A report on these accordingly, including any control deficiencies identified.

3. SCOPE

3.1 The audit included the following scope areas:

- Service Scope – establish the services currently provided by Capita and Littlefish;
- Capita Exit Plan Alignment - Validate completeness of the Capita exit plan based upon the above information;
- Littlefish Risks and Controls – verify that key processes and controls for Littlefish services operate effectively; and
- Reporting and Governance – review service level management processes for Capita and Littlefish. Assess whether the reporting addresses the specified service agreement in place and that the Councils management challenge the provision of services.

3.2 Analysis of the services provided by Littlefish subsequently identified the provision of service request, incident and problem management to be key processes for review by the audit. Other internal audits recently conducted covering Cyber Security and IT Asset Management provide assurance for additional key services provided by Littlefish that were not further tested in this internal audit.

3.3 The audit scope areas and number of observations made is as follows:

Audit Area	Identified Issues		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Capita Exit Plan Alignment	0	0	0
Littlefish Risks and Controls – Service Request Management	0	0	0
Littlefish Risks and Controls – Incident Management	0	0	0
Littlefish Risks and Controls – Problem Management	0	0	0
Littlefish Risks and Controls – Change Management	0	0	1
Reporting and Governance	0	0	1
Totals	**0**	**0**	**2**

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	Whilst 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:

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.

Appendix 3

Statement of Responsibility

We take responsibility to 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 Forvis 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.