MAZARS

CROYDON

Final Internal Audit Report
People ICT Project Audit (Phase 1)
June 2018

Distribution: Director of Residents' and Gateway Services

Interim Director of Gateway and Welfare Services

Assurance Level	Recommendations Made	
	Priority 1	0
Full Assurance	Priority 2	0
	Priority 3	0

Contents

Executive Summary

Appendices

1. Terms Of Reference
2. Definitions For Audit Opinions And Recomendations
3. Statement Of Responsibility

1. Introduction

1.1 The purpose of the "People ICT" project is to develop a fit for purpose, integrated and innovative systems support team. (Separate projects are in place for the procurement of the People's ICT systems, one for pupil data and children and adult social care and the other for housing.) Project documentation indicates that the project will provide consistency and excellence in both daily system support and also help mobilise the delivery of new systems procured.

1.2 The People Department within the Council has a designated responsibility for the management and administration of a number of information systems within specific service areas that are detached (i.e. managed separately) from the Corporate IT Function. These include, Adult Social Care, Children's Services, Education and Housing Management.

1.3 Due to the project not being implemented at the time of the audit, we agreed with the Council that we would audit in two phases and therefore at this stage only phase one was audited. The phases were as follows:

- Phase 1 – January 2018 – to address the first 3 steps of the attached scope in appendix 1, which at a high level covers Strategy, Vision, Governance and the Project itself – i.e. do the plans appear appropriate and is adequate progress being made towards the goals.

- Phase 2 – to address the remaining steps of the attached scope, therefore (a) revisit the observations from Phase 1 above and (b) review the effectiveness of controls designed and implemented as a result of the project's delivery.

1.4 This audit was 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.

2. Areas of good practice

- An approved People ICT Project Business Case (which was last updated on 15 January 2018) was confirmed. The project Business Case clearly illustrates the purpose of the project, problem statement, anticipated benefits, project goals & objectives, project risks, cost benefit analysis for example.
- An approved People ICT Project Initiation Document (PID), which was last updated on 15 January 2018 was confirmed. The PID clearly indicates the project background & purpose, objectives, project deliverables, project approach/scope/key milestones, project governance, project organisation structure and roles & responsibilities, stakeholder analysis and engagement plans for example.
- The People ICT Programme Board was established in April 2017, to act as a vehicle for reviewing the progress of the project, considering and addressing issues, approving budgets and making key decisions throughout. The Programme Board meetings are held at least once every six weeks. Meeting

- minutes and meeting agendas for the last two meeting were inspected and were noted to be effectively covering project issues.
- Project Highlight Reports which provide a snapshot of the current project status are provided by the project team on a monthly basis and shared with other key project stakeholders including the ICT People ICT Programme Board.
- The project organisation structure, roles and responsibilities were clearly defined within the PID. The Head of Gateway Development is the current project sponsor, a project manager was also appointed with clear responsibilities, project team members were identified, and other key stakeholders were also identified with clear roles and responsibilities defined.
- The project was initiated and funded as part of a wider ICT Programme (ICT Systems Procurement Programme) where budgets were approved by the ICT Procurement Programme Board.
- The project risk assessment which identifies key project risks such as, project structural design, project staff recruitment, project transition and project live operations risks is in place and is maintained as and when required by the project team.
- Consultation with affected staff members was regularly undertaken, the last two consultations were carried out in March 2017 and in December 2017. These consultations are important as existing system support staff members are key to the successful delivery of the project.

3.   Key Issues

Examination of the highlight report for 15 January 2018, indicated that the project was delayed due to the revision of the structure and reopening of consultation, plus project staff changes. Project management explained that the project was temporarily delayed and was back on track. The review of the structure and reopening of consultation was necessary as it was critical for existing staff members to be aligned with the direction of the project and their roles and responsibilities.

There were no other key issues identified or recommendations made relating to the audit work carried out.

TERMS OF REFERENCE

Peoples Service ICT

1. INTRODUCTION AND BACKGROUND

1.1 The Peoples Services Department within the Council have a designated responsibility for the management and administration of a number of information systems within specific service areas that are detached from their Corporate IT Function. These include, Adult Social Care, Children's Services, Education and Housing Management.

1.2 The Audit will focus on the newly formed ICT service for the management and support of the IT function within Peoples Services.

1.3 This audit is part of the Internal Audit Plan for 2017/18 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 Peoples Service ICT.

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 associated with the system:

Business Strategy and Business Case

A Business strategy and Business Case for maintaining a separate People Dept. IT unit and for the proposed changes to it, with clear objectives, roles and responsibilities has been approved and is appropriately owned and updated in accordance with the organisation's short, medium and long-term strategies.

Change Project Governance

Appropriate project governance is in place to ensure that the new People Dept. IT unit is delivered on time and within budget, with anticipated savings/ efficiencies being realised and any project variations are subject to appropriate scrutiny and approval.

BAU Management and IT Governance (roles and responsibilities)

An appropriate IT Management and IT Governance (reporting structure, roles and responsibilities) is in place for the continual support and maintenance of security, data processing functions, separation of duties and rotation of responsibilities backed up by appropriate documentation.

IT Security – Policies and Procedures

Responsibility for logical security is appropriately assigned, controlled and communicated, and that these are in accordance with appropriate formal IT/IS policies and procedures. There should also be processes in place to enforce cyber security controls relating to secure configuration, malware defenses and perimeter security.

Logical Access Controls

Controls over logical access applications and data are appropriately controlled through the use of strong passwords, data is encrypted and access is given on a need to know basis. There should also be a process for the creation of new users, deletion of old users and amending access rights where required for systems and applications.

Change Control

Changes to the infrastructure, system and applications are managed and controlled in a consistent manner in accordance with best practice, such as ITIL, and subject to review and authorisation before implementation.

Contingency Planning and Disaster Recovery

There are formal and up-to-date plans in place to cover the restoration of data and IT System and Services that facilitate the continuation of minimal services and the resumption of adequate services within an acceptable time frame.

Legislative Compliance

Policies and procedures cover for legislative compliance against Data Protection, Freedom of Information, Copyright issues and Computer Misuse Acts.

Support and Performance Monitoring

Systems are available and perform as required by the business through the provision of timely and adequate support from the system suppliers and Peoples Service ICT or from Corporate IT and its service provider, Capita, if necessary.

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:

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 represent an exposure to risk and require 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.

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 reply 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.