

Final Internal Audit Report

Information Management

June 2022

Distribution: Interim Assistant Chief Executive
Chief Digital Officer & Director of Resident Access Croydon
Digital Service (Interim)
Head of Corporate Technology
Corporate Director Resources and S151 Officer

Assurance Level	Issues Identified	
Limited Assurance	Priority 1	1
	Priority 2	1
	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, re-interpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, re-interpretation, 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 | |
| Error! Bookmark not defined. | |
| 2. Key Issues | 2 |
-

Detailed Report

- | | |
|---------------------------------------|---|
| 3. Actions and Key Findings/Rationale | 4 |
| 4. Priority 3 Issue | 6 |

Appendices

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

1. Introduction

- 1.1 The Data Protection Act 2018 is the UK's implementation of the European General Data Protection Regulation ('GDPR'). The GDPR came into effect on 25 May 2018, with the intention to strengthen data protection rights for individuals within the EU. This resulted in a need for organisations to review their existing information governance processes and ensure they are robust. Although the list below is not an exhaustive list, below are important aspects of Information Governance:
- Adopting and implementing data protection strategies
 - Appropriate data storage, security, and destruction
 - Staff awareness, understanding and training
 - Suitable Information communication methods
- 1.2 As London Borough of Croydon holds large amounts of data which are sensitive, confidential, and include personal information, it must ensure the data is secure and is not disclosed outside of the organisation besides any official business reasons.
- 1.3 This audit is being undertaken as part of the agreed Internal Audit Plan for 2021/22.

2. Key Issues

- 2.1 The 2020/21 Head of Internal Audit report reported the following Information Governance matter as a significant risk/governance issue, '*Internal audit continues to identify a number of instances where privacy notices relating to the collection of personal data were missing or were no longer fit for purpose*'. The management response provided to this was that, '*We have provided support to service areas in relation to updating or developing new privacy notices so that the council is compliant with GDPR requirements. We have reviewed the below privacy notices between August 2020 to March 2021 Access Croydon, My Account, Corporate privacy notice, Contact Centre privacy notice and Housing Services privacy notices.*'
- 2.2 Discussions with the Information Management Team during the audit confirmed that a privacy notice review timetable was in place. This timetable listed all the services, the proposed review dates, the actual review date as well as the outcome. Review of the proposed and actual review dates confirmed that the first three services due to be reviewed in June 2021 were all completed as planned. Therefore, although work is ongoing, no issue has been raised on this.
- 2.3 Further to this, the following key issues were noted as part of our review:

Priority 1 Issue

The Information Asset Registers (IAR) were not subject to regular review. **(Issue 1)**

Priority 2 Issue

The Information Management Team did not review consent records. **(Issue 2)**

A Priority 3 issue is included under section 4 below.

3. Actions and Key Findings/Rationale

Audit Area: Information Asset Register

Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 1
1	<p>Currently the team where this responsibility lies is being reviewed to build a team that is resilient and able to meet the operational requirements. The current structure does not support proactive work and the ability to make these improvements quickly.</p> <p>Therefore we are looking to embed a new structure by March/ April 22 that will enable a full review of the IAR and update it to be GDPR compliant</p>	<p>Two Information Risk Registers (IARs) are maintained by the Information Management Team (IMT), one for Public Services Provision and one for Corporate Governance. Both IARs contain details of the data held by Croydon Council (Council) including each service. For example, Adult Care Supervision is included and has different assets listed which include client and carer files. In addition, the IARs hold a record of information such as whether the assets have been archived, whether the certification of destruction is held as well as whether the assets have been shared with third parties.</p> <p>However, review of the IARs established that all relevant columns had not been populated, for example, the purpose of many assets is not outlined, the date it was last modified is not recorded or whether a certification of destruction is held.</p> <p>The Head of Legal Business and Compliance stated the IARs have not been reviewed since 2018. We were informed the matter has been added to the Information Management improvement plan to ensure the IARs are reviewed on an annual basis.</p>
<p>Responsible Officer</p>	<p>Deadline</p>	<p>Where the IARs are incomplete, there is risk the Council does not have all of the necessary information to ensure subjects’ data is obtained, processed, and retained appropriately, this can result in reputational and financial damage. Where the IARs are not subject to periodic reviews, there is a risk that the Council does not fully understand what information is held, and therefore is unable to protect it. This could therefore lead to an increased number of data breaches and cases being escalated to the Information Commission Office (ICO), resulting in financial penalties.</p>
<p>Head of Corporate Technology</p>	<p>April 2022</p>	

Audit Area: Data Collection and Data Retention

Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 1
2	The responsibilities and function of the new team will take this into consideration and strengthen the way in which LBC review consent records. Therefore this will be improved by August 2022 once the new team structure is fully embedded	<p>Discussion with the Acting Information Manager established that the IMT did not manage consent records as these were kept with the relevant service areas and therefore, reviews of consent records were not undertaken by the IMT.</p> <p>Where regular reviews of consent records are not undertaken by the IMT/and or service area there is a risk the records maintained do not adequately meet the requirements of the GDPR, whereby these do not highlight when and how the consent was obtained. Moreover, the IMT cannot establish whether the relationship, the processing and the purpose of the information have changed over time. This can lead to action being taken against the Council by the Information Commission’s Office (ICO).</p>
Responsible Officer	Deadline	
Head of Corporate Technology	August 2022	

4. Priority 3 Issue

Action Proposed by Management	Detailed Finding/Rationale
<p>Management Information and Reporting</p> <p>1) The roles and responsibilities of the information management function is being reviewed in line with the attached plan. The team structure is being reviewed in March/ April which will be when the IMSG or governance group will also be reviewed and reinstated. Currently the ToR and members of this group is undetermined so please note the attached plan which will be able to review and assure this audit.</p> <p>Currently the Data Breach panel meet to cover off high risks and concerns but it is noted and agreed that there needs to be a wider forum for corporate risks to be discussed and mediated, with escalation to senior management.</p> <p>...an update will be provided as part of the Mar review.</p>	<p>There is an Information Management Steering Group (IMSG) in place who meet on a bi-monthly basis, to ensure the Council meet their obligations with regards to Information Management.</p> <p>The requested Terms of Reference for the IMSG has not been provided therefore, no control testing has been completed to establish whether the responsibilities of the Group are clearly defined.</p> <p>Internal Audit have therefore not been able to express an assurance opinion in this area as we have not been able to obtain sufficient evidence to provide a basis for an audit opinion.</p>

AUDIT TERMS OF REFERENCE

Information Management – 2021/22

1. INTRODUCTION & BACKGROUND

- 1.1 The Data Protection Act 2018 is the UK’s implementation of the European General Data Protection Regulation (‘GDPR’). The GDPR came into effect on 25 May 2018, with the intention to strengthen data protection rights for individuals within the EU. This resulted in a need for organisations to review their existing information governance processes and ensure they are robust. Although the list below is not an exhaustive list, below are important aspects of Information Governance:
- Adopting and implementing data protection strategies
 - Appropriate data storage, security, and destruction
 - Staff awareness, understanding and training
 - Suitable Information communication methods
- 1.2 As London Borough of Croydon holds large amounts of data which are sensitive, confidential, and include personal information, it must ensure the data is secure and is not disclosed outside of the organisation besides any official business reasons.
- 1.3 This audit is being undertaken as part of the agreed Internal Audit Plan for 2021/22.

2. AUDIT OBJECTIVES AND METHODOLOGY

- 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 for each controls / process being considered:
- Walkthrough the processes to consider the key controls;
 - Conduct sample testing of the identified key controls, and
 - Report on these accordingly.

3. SCOPE

3.1 The audit included the following areas (and number of issues raised):





Audit Area	Identified Issues		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Legislative, Organisational and Management Requirements	0	0	0
Data Collection and Data Retention	0	1	0

Audit Area	Identified Issues		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Information Asset Register	1	0	0
Data Breaches and Losses	0	0	0
Management Information and Reporting	0	0	1
Totals	1	1	1

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:

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.

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.