

Final Internal Audit Report

Legal Services Case Management System

November 2024

Distribution: Interim Assistant Chief Executive
Corporate Director of Resources & S151 Officer
Interim Chief Digital Officer & Director of Resident Access
Director of Legal Services & Monitoring Officer
Head of Corporate Technology (Interim)
Head of Business Compliance and Legal
Data Protection Officer (DPO)
Director of Finance (Deputy S151)

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

[Confidentiality and Disclosure Clause](#)

This report ("Report") was prepared by Forvis 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 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. 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**

| | |
|-----------------|---|
| 1. Introduction | 3 |
| 2. Key Issues | 3 |

Detailed Report

| | |
|---------------------------------------|---|
| 3. Actions and Key Findings/Rationale | 4 |
| 4. Priority 3 issues | 7 |

Appendices

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

1. Introduction

- 1.1 The Legal Services directorate is responsible for handling legal cases that arise from each of the council's services (social care, housing, procurement etc). To support the assessment of each case, and the collation and presentation of evidence to court, a case management system from Nexis Lexis called Visual Files is used.
- 1.2 Whilst the system has add-ons to support integrations with Outlook, and to support the collaboration and sharing of evidence, it is effectively self-contained and thus does not exchange information with other IT systems within the Council.
- 1.3 The application relies on a Progress database hosted in Azure where it can be accessed either through Citrix, or via local installations on standalone desktops. Access to the system is limited to legal personnel within Croydon Council.
- 1.4 The system is owned by the Head of Legal Business and Compliance, and it is supported by Digital Operations Services.
- 1.5 This audit is being undertaken as part of the agreed Internal Audit Plan for 2022/23.

2. Key Issues

Priority 2 Issues

There is lack of data or information assets classification for Visual Files (VF), posing the risk of unauthorised access, misuse, or disclosure. **(Issue 1)**

There was no data protection impact assessment (DPIA) for VF, leading to the potential risk of data breaches, financial losses, and reputational damage. **(Issue 2)**

Two 'Priority 3' issues are included under Section 4 below.

3. Actions and Key Findings/Rationale

Audit Area: Application Management and Governance

| Priority | Action Proposed by Management | Detailed Finding/Rationale - Issue 1 |
|----------|---|--|
| 2 | <p>A classification document has been drafted by the new Head of Legal Business with a view to consulting with the legal teams and finalising by 31 March 2024.</p> <p>Access Plans have also been prepared for Visual Files and this will be implemented as a priority into the system as part of the recently initiated Visual Files improvement project.</p> <p>This should be considered as a corporate issue rather, with CDS leading, than one for Legal Service, save for the eventual updating of VF with a Classification Scheme, once corporately agreed and implemented.</p> | <p>Expected Control</p> <p>Personal and/or sensitive data processed by the application has been identified, classified, and communicated to Council's Data Protection Officer.</p> <p>The 'Information Management Policy' requires that Council information is assigned an information classification of Official.</p> <p>Information classification is a process in which organisations assess the data that they hold and the level of protection it should be given. According to 'ISO/IEC 27001:2022¹ – Information Security Management', information should be adequately protected in accordance with its significance to the organisation (and interested parties such as customers).</p> <p>Finding/Issue</p> <p>Discussion with management noted that, despite the policy, information classification was not implemented across the Council. There was no data or information asset classification performed for the Visual Files (VF) application (that supports the legal services case management process.)</p> <p>Risk</p> <p>In the absence of the information asset classification recipients of information produced from the Visual Files (VF) application may not take adequate precautions to protect information, increasing the likelihood of data loss in the event of a security breach.</p> |
| | <p>Responsible Officer</p> <p>Deadline</p> | |

¹ [https://www.isms.online/iso-27001/annex-a-8-asset-management/#:~:text=ISO%2027001%3A2013%3F-,Annex%20A.,interested%20parties%20such%20as%20customers\).](https://www.isms.online/iso-27001/annex-a-8-asset-management/#:~:text=ISO%2027001%3A2013%3F-,Annex%20A.,interested%20parties%20such%20as%20customers).)

LBC Final Audit Report – Legal Services Case Management System Review 2022-23

| | | |
|------------------------|--------------|--|
| Head of Legal Business | 30 June 2024 | |
|------------------------|--------------|--|

Audit Area: Application Management and Governance

| Priority | Action Proposed by Management | Detailed Finding/Rationale - Issue 2 | | | | |
|------------------------|--|---|----------|------------------------|--------------|--|
| 2 | DPIA has been prepared and will be reviewed at least annually by the Head of Legal Business in collaboration with the Information Governance Coordinator and CDS. | <p>Expected Control</p> <p>Personal and/or sensitive data processed by the application has been identified, classified, and communicated to the Council's Data Protection Officer.</p> <p>Data Protection Impact Assessments (DPIAs) are an important tool to identify, assess, and mitigate the potential risks associated with the processing of personal data.</p> <p>Finding/Issue</p> <p>Discussion with the Data Protection Officer (DPO) was noted that a Data Protection Impact Assessment (DPIA) exercise had not been undertaken for the VF application. Additionally, it was also noted the Council did not have a defined process for this and it was still being defined.</p> <p>Risk</p> <p>Failure to carry out a DPIA when required may leave the Council open to enforcement action, including a fine of up to £8.7 million, or 2% global annual turnover if higher², if personally identifiable information is found to not be adequately controlled in the event of a data breach.</p> | | | | |
| | <table border="1"> <thead> <tr> <th>Responsible Officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>Head of Legal Business</td> <td>30 June 2024</td> </tr> </tbody> </table> | Responsible Officer | Deadline | Head of Legal Business | 30 June 2024 | |
| Responsible Officer | Deadline | | | | | |
| Head of Legal Business | 30 June 2024 | | | | | |

² <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/penalties/>

4. Priority 3 Findings

Audit Area: Change Management Control

| Agreed action | Findings |
|---|---|
| <p>Control Area 1: Change testing / validation documentation</p> <p><u>Action proposed by management:</u></p> <p>CDS accepts that on this occasion an email did not close the CAB process loop as described in the workflow; it was on the day as the audit pointed out agreed in the CAB meeting that an email stating that the testing would be completed would suffice. Going forward the workflow will be adhered to.</p> <p>Management will ensure all relevant approvals are obtained prior to the changes being implemented.</p> <p><u>Responsible Officer:</u></p> <p>Interim Product and Support Manager / Head of Legal Business</p> <p><u>Deadline:</u></p> <p>Immediate</p> | <p>Expected Controls</p> <p>Changes are adequately tested and are authorised before release to production.</p> <p>Finding/Issue</p> <p>In December 2022, the VF application underwent a new change, related to e-bundles, to apply to all hearings after January 1, 2023. For this, a change request was raised on 1 December 2022 to accommodate the upgrade required.</p> <p>Based on the information on the Service Desk log, it is noted that testing was performed on 12 January 2023, and emails containing communications on testing being performed and validated by business users were also obtained.</p> <p>Whilst this evidence demonstrated that testing had been performed, it did not provide clear acceptance that the outcome of testing performed was sufficient to implement the change.</p> <p>Risk</p> <p>Emails may not provide clear acceptance from business stakeholders that the outcome of testing supports the promotion of changes to production.</p> |
| <p>Control Area 1: Change Advisory Board (CAB) Approval</p> <p><u>Action proposed by management:</u></p> | <p>Expected Control</p> <p>The software management policy defines the correct processes and procedures to be followed when purchasing, developing, deploying, maintaining and replacing software applications. The policy requires that major changes to applications and operating system software must be subject to change management procedures</p> |

| Agreed action | Findings |
|---|---|
| <p>CDS accepts that on this occasion an email did not close the CAB process loop as described in the workflow; it was on the day as the audit pointed out agreed in the CAB meeting that an email stating that the testing would be completed would suffice. Going forward the workflow will be adhered to.</p> <p>Management will ensure all relevant approvals are obtained prior to the changes being implemented.</p> <p><u>Responsible Officer:</u> Interim Product and Support Manager / Head of Legal Business</p> <p><u>Deadline:</u> Immediate</p> | <p>before being implemented to ensure that any risk to business continuity and system availability is mitigated. The procedures include:</p> <ul style="list-style-type: none"> ▪ maintenance of an audit trail of all change requests; and ▪ obtaining formal approval for the proposed work prior to commencement. <p>Finding/Issue</p> <p>It was noted that a recent change / modification was made to the VF application in December 2022, based on the change in Practice Direction relating to e-bundles.</p> <p>Examination of the meeting minutes of Croydon's Change Advisory Board (CAB) meeting on 7 December 2022 was unable to locate a decision of approval being made for this change. It was further documented that the approval was obtained from the appropriate or authorised individuals, but it was done outside of the CAB process.</p> <p>Management should consider obtaining and documenting any supplementary approvals prior to the CAB meeting. This will ensure that any changes are properly reviewed and approved, and that any potential risks are identified and addressed before the changes are implemented.</p> <p>Risk</p> <p>Without obtaining and documenting the approval from the Change Advisory Board (CAB) for changes to Croydon's IT systems and processes, changes could have unintended consequences and cause disruption to their operations.</p> |

AUDIT TERMS OF REFERENCE

Legal Services Case Management System

1. INTRODUCTION

- 1.1 The Legal Services directorate are responsible for handling legal cases that arise from each of the council's services (social care, housing, procurement etc). To support the assessment of each case, and the collation and presentation of evidence to court, a case management system from Nexus Lexus called Visual Files is used. Whilst the system has add-ons to support integrations with outlook, and to support the collation and sharing of evidence, it is effectively self-contained and thus does not exchange information with other council IT systems.
- 1.2 The application relies on a Progress database hosted in Azure. The application can be accessed either through Citrix, or via local installations on standalone desktops.
- 1.3 A proposal to add a further module to support cross charging of legal fees to the directorates from which cases originate is on-hold. A request to acquire this add-on was declined by the council's procurement team, as due to the age of the system, they have determined that a retender for the supply of the service should first occur.
- 1.4 In addition, management are aware of several risks in relation to the operation of the system such as:
 - Internal support relies on one key individual;
 - Legal services do not have their own trained staff to generate reporting and thus despite the above constraint, rely on IT for this;
 - Frequent staff movements in legal services may mean that there are few trained users of the system;
 - Teams in legal services are known to follow different working practices in relation to the system yet the system has not been customised to their needs; and,
 - Excess incidents arise due to the use of the system within Citrix, and due to issues with residual components of earlier MS Office tools on laptops that have local installations of Visual Files.
- 1.5 This audit was undertaken as part of the agreed Internal Audit Plan for 2022/23.

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 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 a number of issues identified):

| Audit Area | Identified Issues | | |
|---------------------------------------|-------------------|---------------------|------------------|
| | Priority 1 (High) | Priority 2 (Medium) | Priority 3 (Low) |
| Application Management and Governance | 0 | 2 | 0 |
| System Security | 0 | 0 | 0 |
| Data Input, Output and Processing | 0 | 0 | 0 |
| Change Control | 0 | 0 | 2 |
| System Resilience and Recovery | 0 | 0 | 0 |
| Totals | 0 | 2 | 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 | 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 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