Leeds City Council

Data protection audit report

December 2023

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Leeds City Council (LCC) agreed to a consensual audit of its data protection practices in June 2023. ICO audit team managers completed a scoping call with LCC to further discuss their current data protection compliance levels and the appropriate scope areas on which to focus the audit.

The purpose of the audit is to provide the Information Commissioner and LCC with an independent assurance of the extent to which LCC, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of LCC's processing of personal data. The scope may take into account any data protection issues or risks which are specific to LCC, identified from ICO intelligence or LCC's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of LCC, the nature and extent of LCC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to LCC.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate.

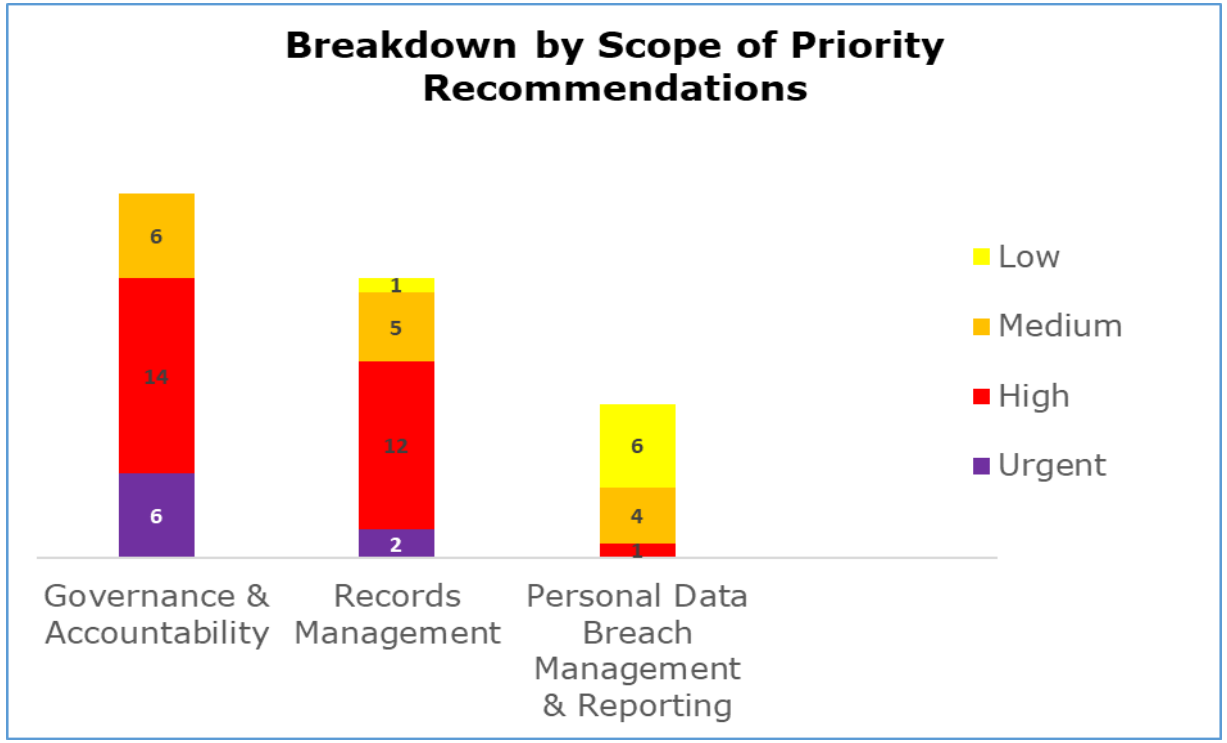
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential documentation.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist LCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. LCC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Personal Data Breach Management and Reporting	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

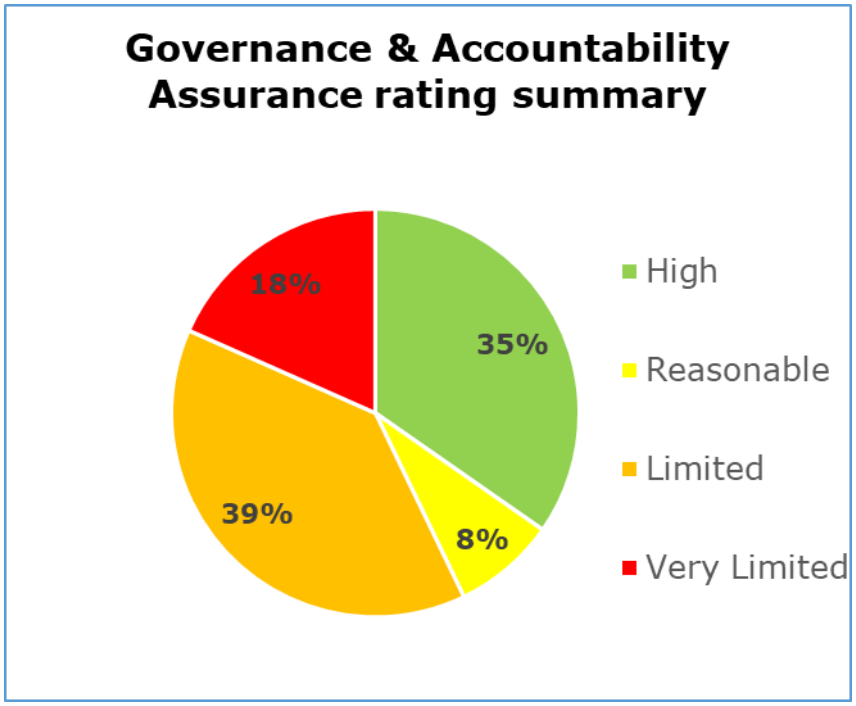
Priority Recommendations



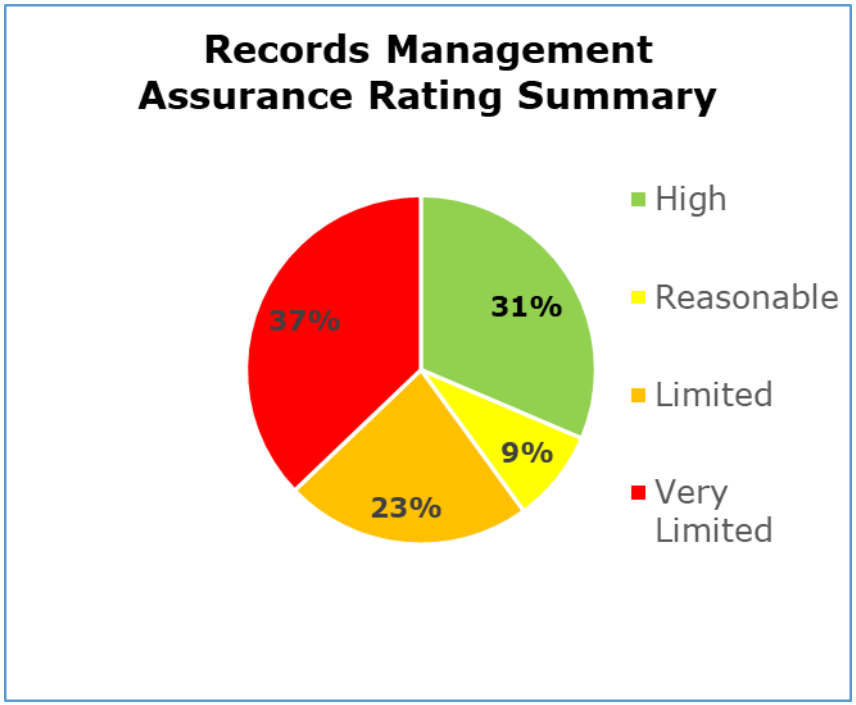
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has six urgent, 14 high, six medium and no low priority recommendations.
- Records Management has two urgent, 12 high, five medium and one low priority recommendation.
- Personal Data Breach Management and Reporting has no urgent, one high, four medium and six low priority recommendations.

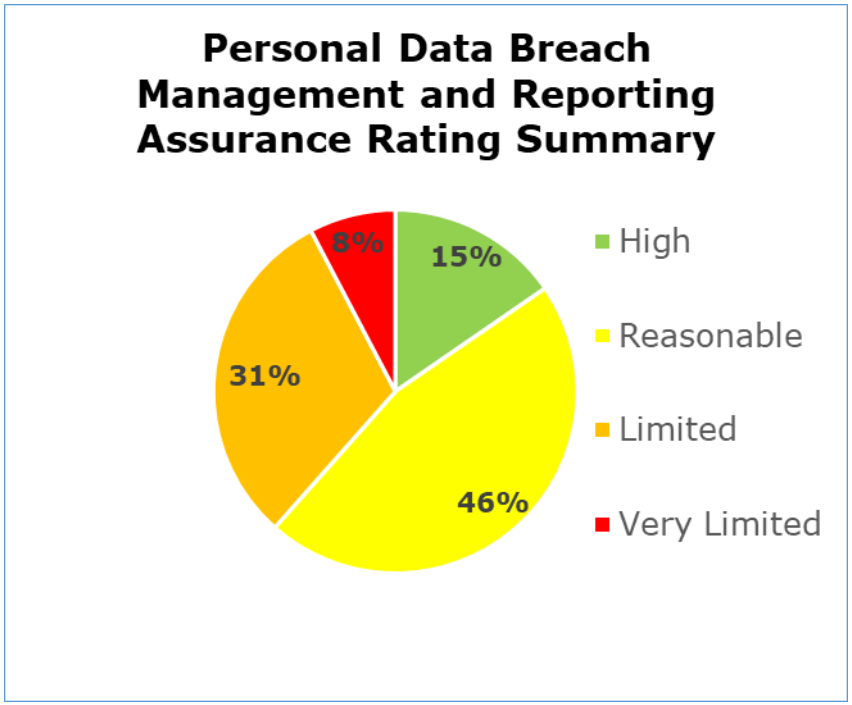
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 35% high assurance, 8% reasonable assurance, 39% limited assurance, 18% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 31% high assurance, 9% reasonable assurance, 23% limited assurance, 37% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management and Reporting scope. 15% high assurance, 46% reasonable assurance, 31% limited assurance, 8% very limited assurance.

Areas for Improvement

Governance and Accountability:

- LCC must review, update, and create any missing Data Protection (DP) and Information Governance (IG) policies. These documents should be suitably extensive for the context of LCC and provide staff with sufficient direction that they are able to identify their roles and responsibilities.
- LCC should create an internal audit programme specific to DP with oversight and input from the Data Protection Officer (DPO). By implementing internal DP audits, LCC can gain assurance that their risk management is effective.
- LCC must create a centralised records of processing activities (RoPA) document. This will ensure LCC are in compliance with UK GDPR Article 30.
- LCC must conduct a review of their privacy notices to ensure that they include all the information required under Articles 13 & 14 of the UK GDPR. This will ensure that privacy information is sufficient to meet the legal requirements.

Records Management:

- LCC must complete an information audit and use it to inform their information asset register (IAR), RoPA and a weeding schedule and guidance. Without this, they cannot be assured they have full visibility of their information assets or the data quality of the assets.
- Disposal of excessive records is critical to UK GDPR compliance. LCC must create a full and relevant retention schedule and ensure there are sufficient processes in place to make sure this is enacted.

- LCC should ensure they have full and clear visibility of where data sharing has taken place and that appropriate contracts are in place. This will help processing of individual rights requests efficiently.
- There aren't consistent approaches to records management across the whole council which means that there's a risk of poor practice due to lack of clear guidance. Policies and guidance related to Records Management must be reviewed to ensure they are clear and cover everything required.

Personal Data Breach Management and Reporting:

- LCC should ensure that all decision makers within the IG team have received specialised training on Personal Data Breach Management and Reporting. This will ensure breaches are being accurately assessed and reported to the ICO where necessary.
- LCC should update the overarching retention documents to include retention periods, procedures and data minimisation techniques for the data breach logs. This will help LCC have an awareness of how often they should review breach logs and periodically reduce the personal information held within them.
- LCC should implement an alternate notification route in the case of a data breach that has been reported out of office hours. This will ensure that the council have appropriate procedures and guidance in place to maintain compliance.
- LCC should ensure all discussions held verbally or via email regarding reporting PDBs to the ICO are documented, e.g. decisions over not reporting a PDB to the ICO, the reason for any delays and any advice received from the supervisory authority.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Leeds City Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Leeds City Council. The scope areas and controls covered by the audit have been tailored to Leeds City Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.