London Borough of Waltham Forest Council

Data protection audit report

July 2021

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 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

London Borough of Waltham Forest Council (LBWF) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 17 March 2021 with representatives of LBWF to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and LBWF with an independent assurance of the extent to which LBWF, 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 LBWF's processing of personal data. The scope may take into account any data protection issues or risks which are specific to LBWF, identified from ICO intelligence or LBWF's own concerns, and/or any data protection issues or risks which affect their 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 LBWF, the nature and extent of LBWF's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to LBWF.

It was agreed that the audit would focus on the following areas:

Scope area	Description
Governance & 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.
Freedom of Information (FOI)	The extent to which FOI accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

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

However, due to the Covid -19 pandemic this methodology was no longer appropriate. Therefore, LBWF agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 10 – 20 May 2021. The ICO would like to thank LBWF for its flexibility and commitment to the audit during difficult and challenging circumstances.

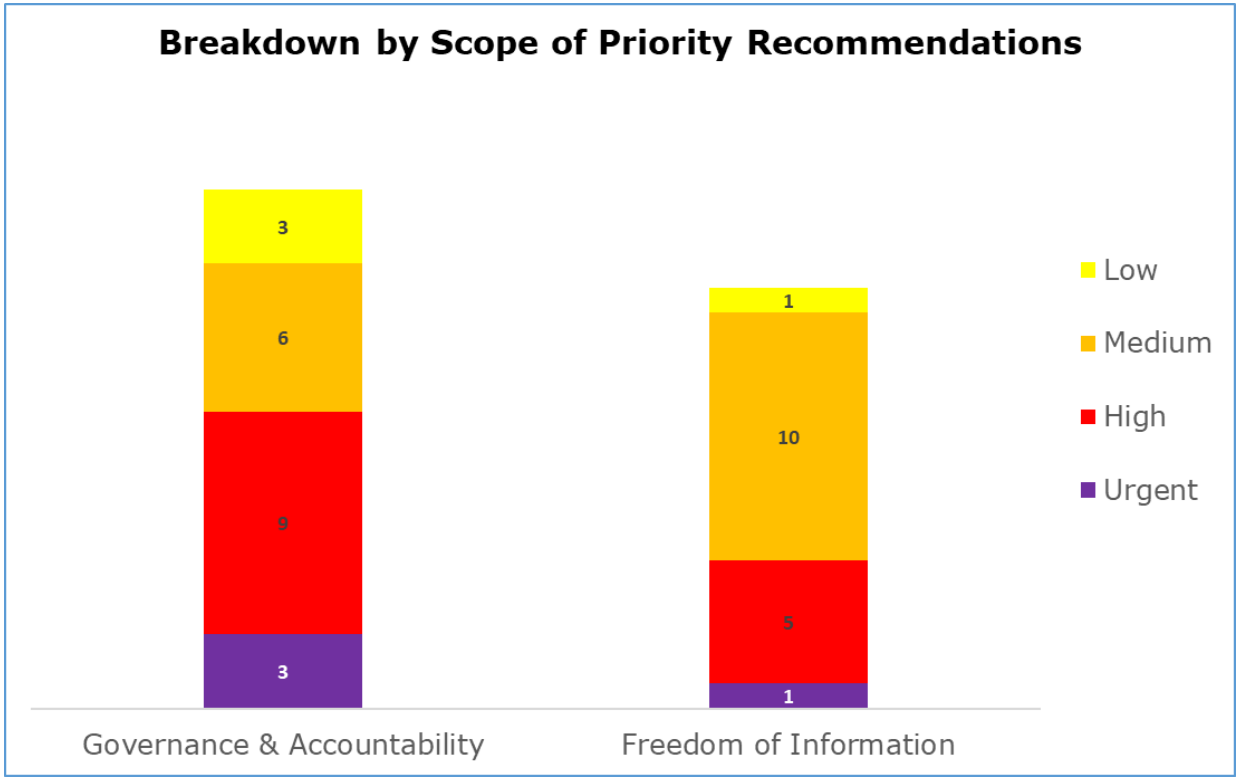
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist LBWF in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. LBWF'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 & 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.
Freedom of Information	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 freedom of information legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

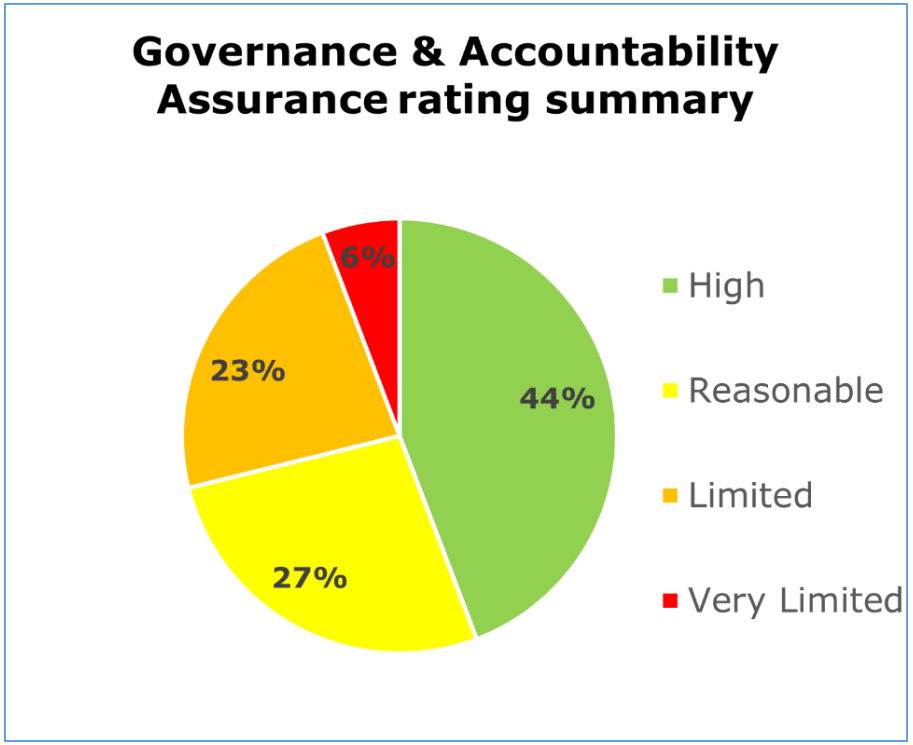
Priority Recommendations



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

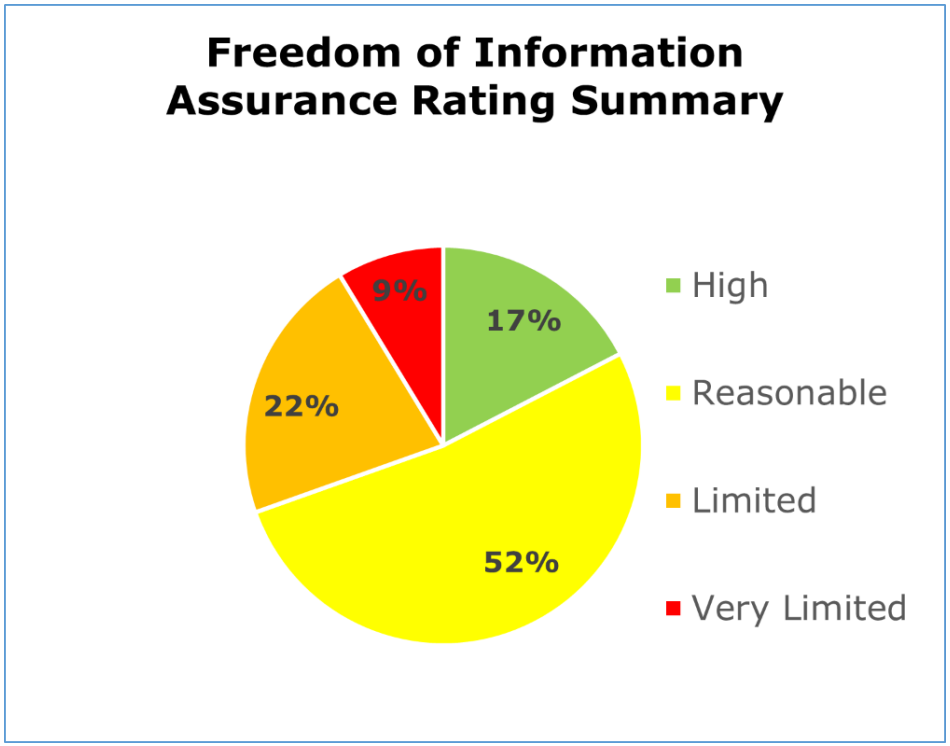
- Governance & Accountability has 3 urgent, 9 high, 6 medium and 3 low priority recommendation.
- Freedom of Information has 1 urgent, 5 high, 10 medium and 1 low priority recommendation.

Graphs and Charts



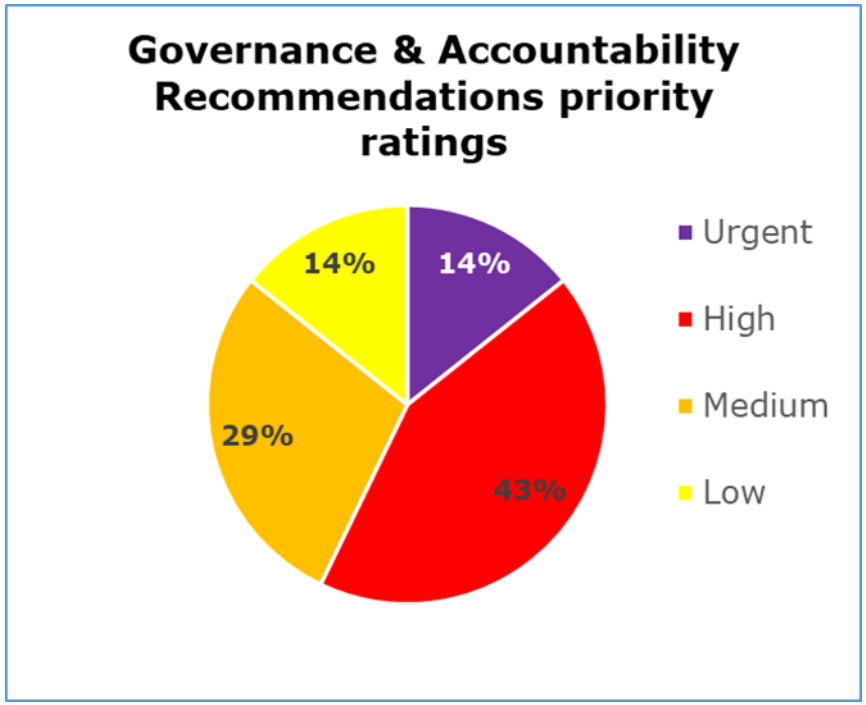
The pie chart shows the percentage breakdown of the assurance ratings given for the Governance and Accountability scope:

- 44% high assurance
- 27% reasonable assurance
- 23% limited assurance
- 6% very limited assurance



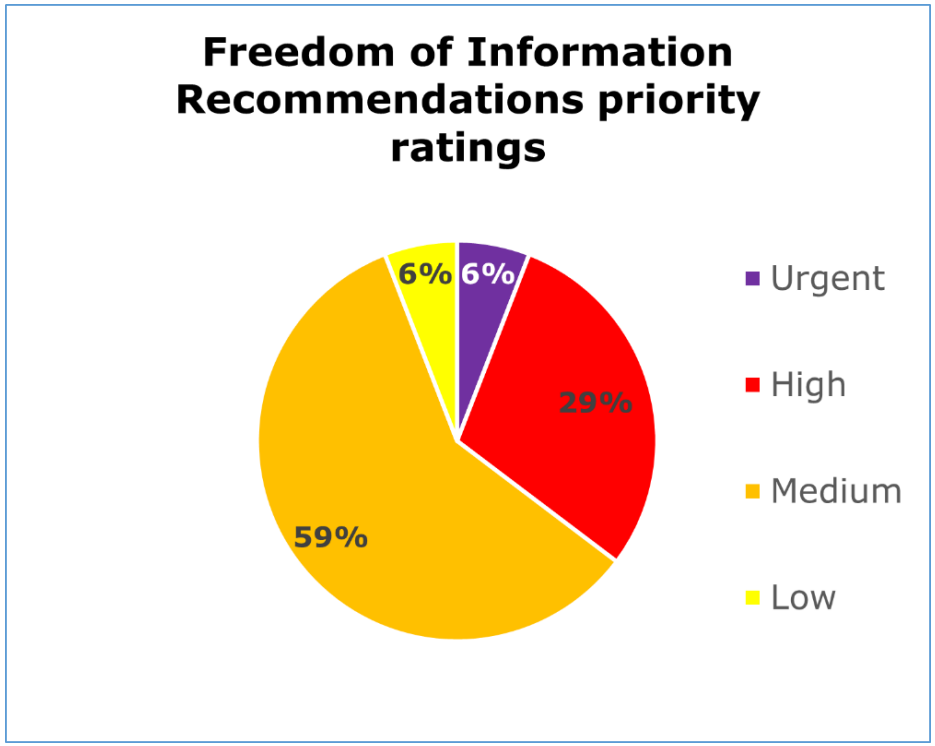
The pie chart shows the percentage breakdown of the assurance ratings given for the Freedom of Information scope:

- 17% high assurance
- 52% reasonable assurance
- 22% limited assurance
- 9% very limited assurance



The pie chart shows a summary of the priority ratings assigned to the recommendations made in the Governance and Accountability scope:

- 14% urgent priority
- 43% high priority
- 29% medium priority
- 14% low priority



The pie chart shows a summary of the priority ratings assigned to the recommendations made in the Freedom of Information Scope:

- 6% urgent priority
- 29% high priority
- 59% medium priority
- 6% low priority

Areas for Improvement

- LBWF should consider reassigning its DPO position or putting an alternative reporting structure in place for LBWF's deputy DPO to take the lead on matters which could be perceived as a conflict of interest for its DPO.

- LBWF does not currently report KPIs on its compliance with subject access requests or records management obligations. By not monitoring this data LBWF lacks oversight and assurance that it is in compliance with its statutory obligations. LBWF should begin capturing and monitoring this data on a routine basis.

- LBWF does not currently have sufficient oversight on all the contracts it has in place with data processors. LBWF should create a central log of the contracts it has in place to ensure that all contracts in place are accounted for and monitored as needed.

- LBWF does not have any standard due diligence checks built into its procurement process prior to engaging in the services of a processor. LBWF should implement a set of standard checks as part of its procurement process to ensure that its processors are all meeting UK GDPR requirements and protecting data subjects' rights.

- The Information Governance Board should monitor the completion rates of all staff FOI training and specialist training (at both induction and refresher stages). This will help LBWF provide assurance that all staff have received the correct training.

- A cold case FOI quality assurance process should be established. Periodic reviews of cold case FOI requests should be checked and results recorded and feedback provided to IGB and the individuals involved in the original request.

- LBWF should ensure that all staff receive at least a basic level of training on FOI and EIR requests. Training should cover what a request is, how a request may be received (i.e., can be via social media, EIR requests can be verbal), the fact the request doesn't need to reference the legislation and what to do if they receive a request. This training should be mandatory for all staff and be refreshed on a regular basis.

Best Practice

- LBWF have incorporated videos into the privacy notice section of its website to provide privacy information in a different format that may be more accessible to individuals.

- LBWF effectively monitor adherence to statutory timescales for FOI and EIR requests via Executive Assistants and daily and weekly reporting mechanisms.

- All staff interviewed showed a good understanding and knowledge of the LBWF FOI Procedure.

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 London Borough of Waltham Forest 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 London Borough of Waltham Forest Council. The scope areas and controls covered by the audit have been tailored to London Borough of Waltham Forest Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.