Wakefield Council

Data protection audit report

September 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.

Wakefield Council has agreed to a consensual audit by the ICO of its processing of personal data.

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

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

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	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.
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

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 outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, WC 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 14 September 2021 to 16 September 2021. The ICO would like to thank WC 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 WC 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. WC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

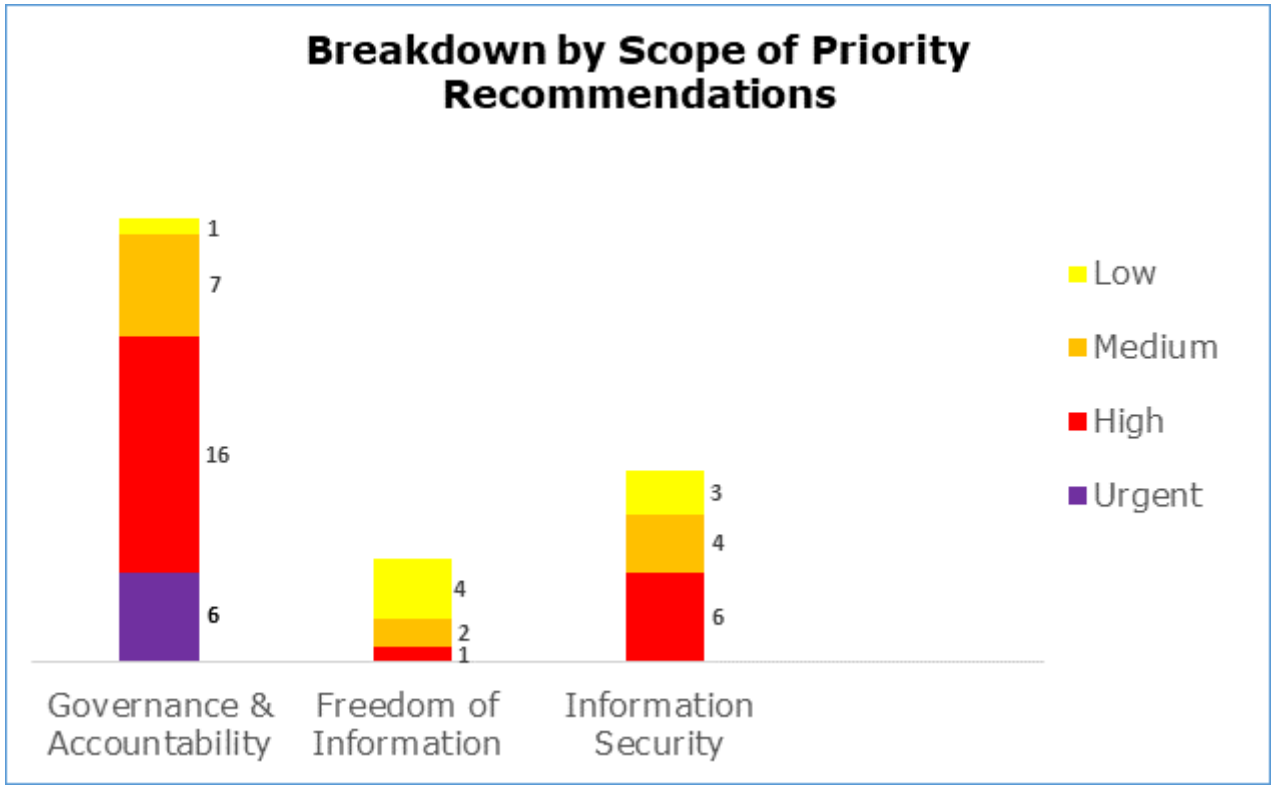
Audit Summary

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	High	There is a high level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with freedom of information legislation.
Information Security	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.

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

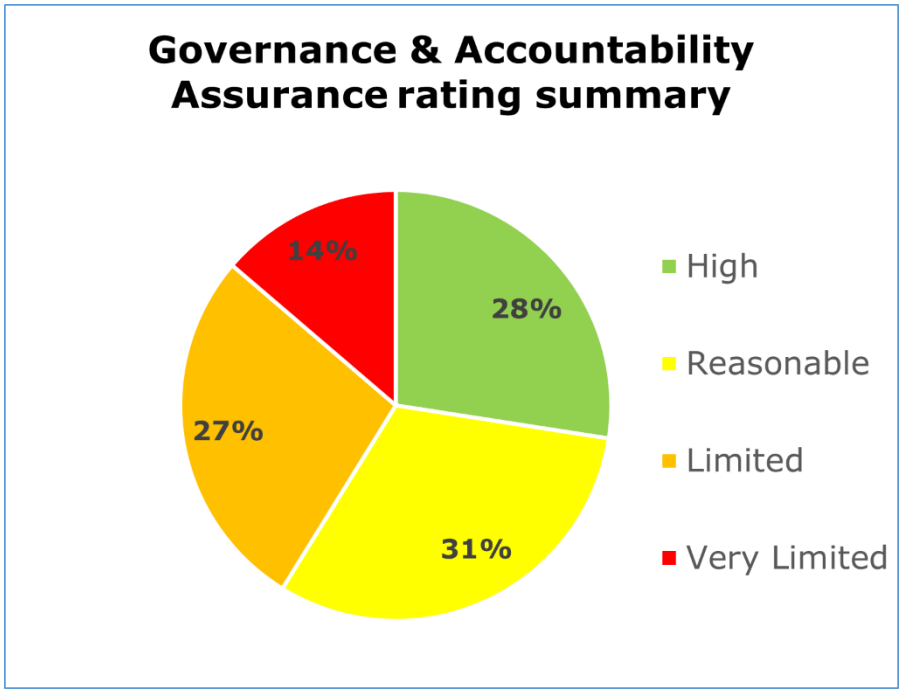
A bar chart showing a breakdown by scope area of the priorities assigned to the recommendations made.



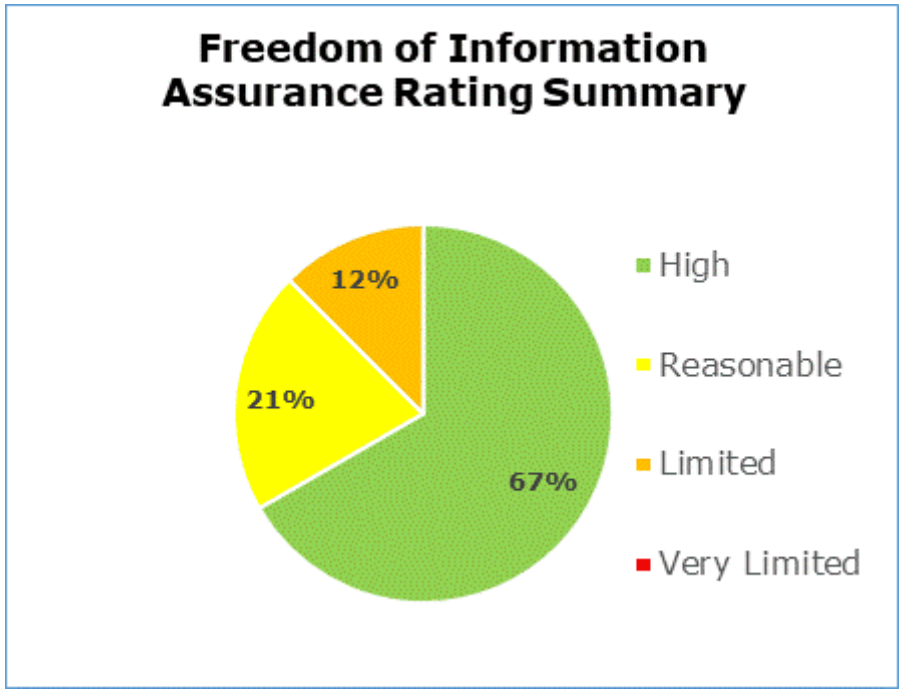
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has six urgent, 16 high, seven medium and one low priority recommendations
- Freedom of Information has one high, two medium and four low priority recommendations
- Information Security has six high, four medium and three low priority recommendations

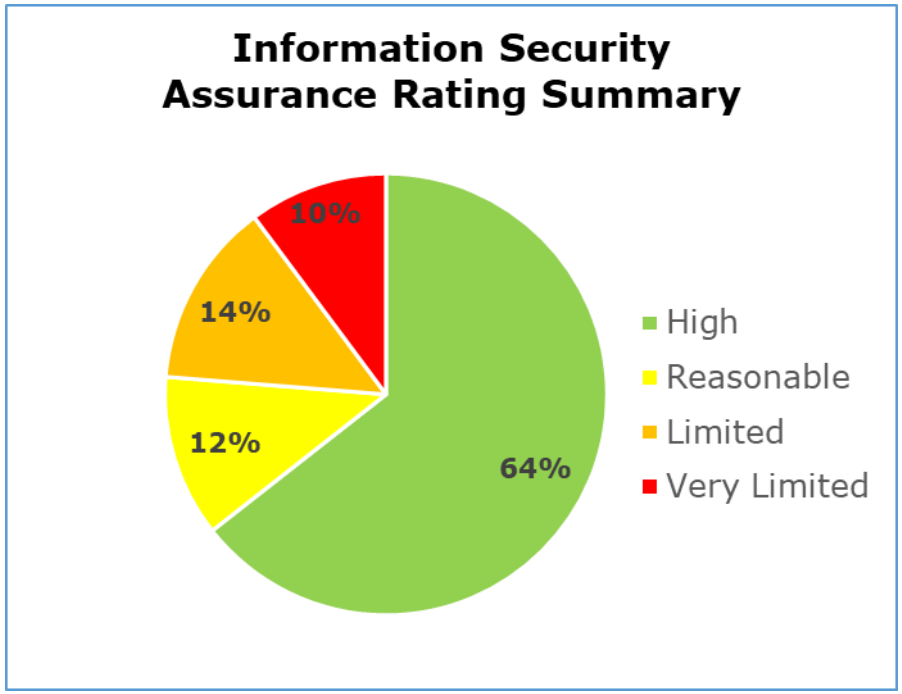
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 28% high assurance, 31% reasonable assurance, 27% limited assurance, 14% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 67% high assurance, 21% reasonable assurance, 12% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Security scope. 64% high assurance, 12% reasonable assurance, 14% limited assurance and 10% very limited assurance.

Areas for Improvement

- WC does not currently have an Information Risk Register. An Information Risk Register should be introduced to enable WC to formally document areas of information risk in each directorate and allow them to comprehensively review the risks attached. This will ensure WC are taking adequate steps to mitigate information risk.
- The Appropriate Policy Document (APD) for WC does not set out the specific Schedule 1 or Schedule 8 conditions for processing. WC should update its APD to ensure it incorporates the relevant conditions for processing, to ensure sufficient consideration has been given to their bases for processing of special category data.
- WC's combined FOI/EIR and DP training in one module may well confuse staff when working with the legislation(s). In addition, the training does not specifically advise on what steps should be taken when receiving a verbal EIR request. This could lead to non-compliance in either Data Protection or FOI legislation.
- Whilst FOI policies and procedures are in place, some of the documents are out of date and need updating to reflect current WC practice.
- Information security training is currently not mandatory and there is no test or assessment at the end of the training to help check staff's understanding of information security and how it impacts their roles.
- WC need to develop processes that give them greater oversight of service areas line of business applications.

Best Practice

- A group of WC's GDPR Champions collaborate to produce a weekly GDPR bulletin email for their directorate. The bulletin consists of both standing items to serve as a reminder for their colleagues of key points they need to be mindful of at all times, and a short case study or summary on a particular topic or theme.
- The Principal Information Governance Officers have used the pandemic as an opportunity to transform the way their Data Security and Information Sharing training is delivered to staff. They have recorded a narrative to go alongside a slideshow, in lieu of delivering in-person or live online training. This means staff are able to complete the training at a convenient time, and can break it up into smaller sections if required without the need to interrupt or redo a training session. It also reduces the demand on CIGT staff time as they do not have to be available to present training - freeing up resources to be utilised within the CIGT.

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