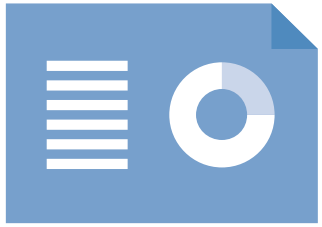
Gloucestershire County Council

Data protection audit report

October 2020

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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.

Gloucestershire County Council (GCC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 2 July 2020 with representatives of GCC to discuss the scope of the audit.

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

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 GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security (Security of Personal Data)	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity, and availability of manually and electronically processed personal data.
Freedom of Information (FOI)	The extent to which FOI/EIR 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 outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, GCC 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 10-27 August 2020. The ICO would like to thank GCC for its flexibility and commitment to the audit during difficult and challenging circumstances.

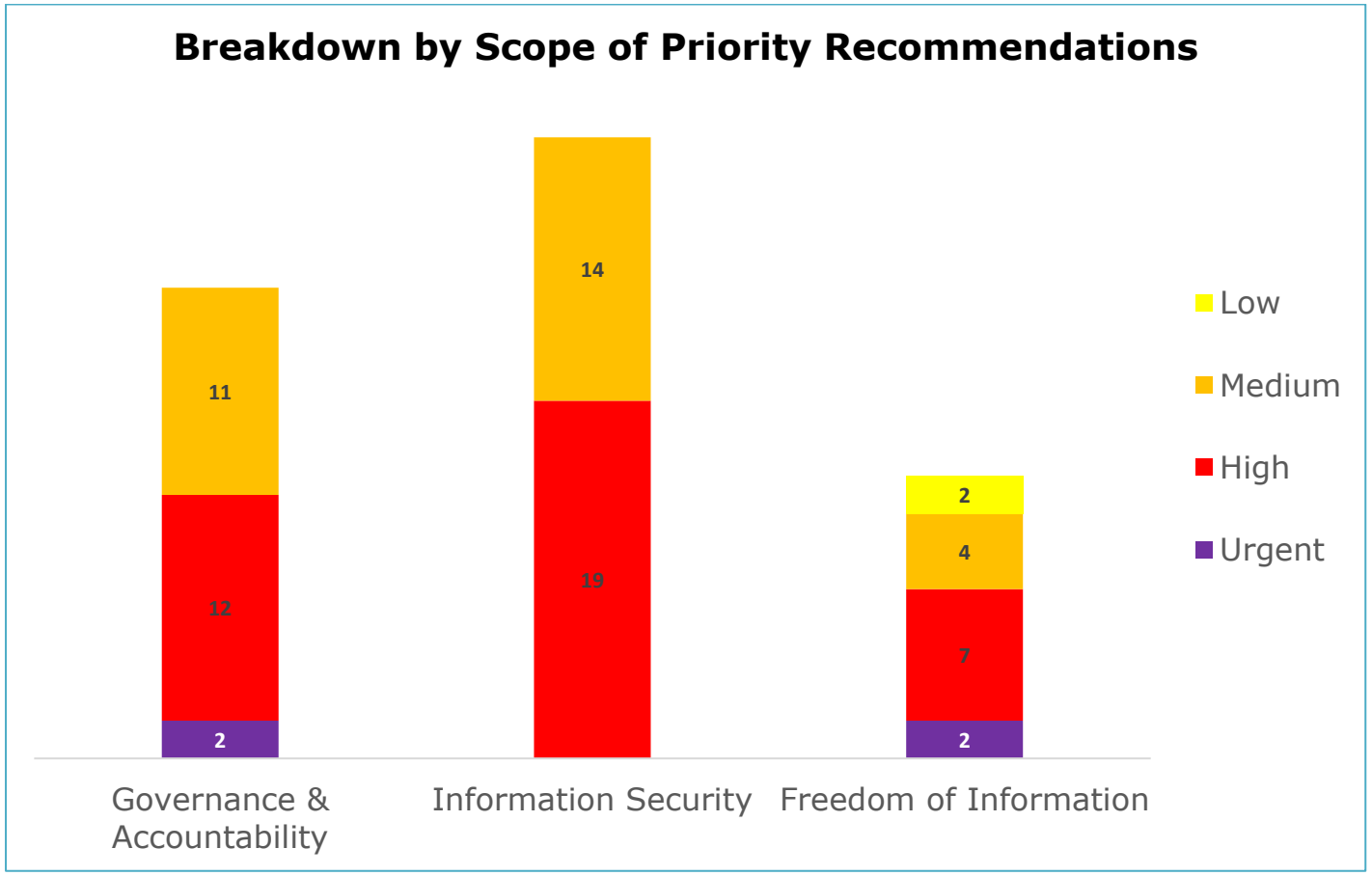
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist GCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they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

Audit Summary*

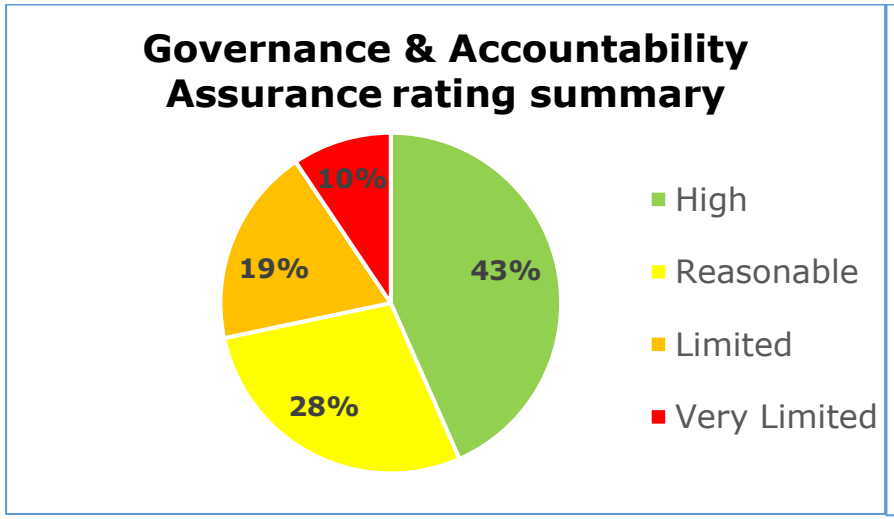
Audit Scope Area	Audit Scope Area	Audit Scope Area
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
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.
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 data protection legislation.

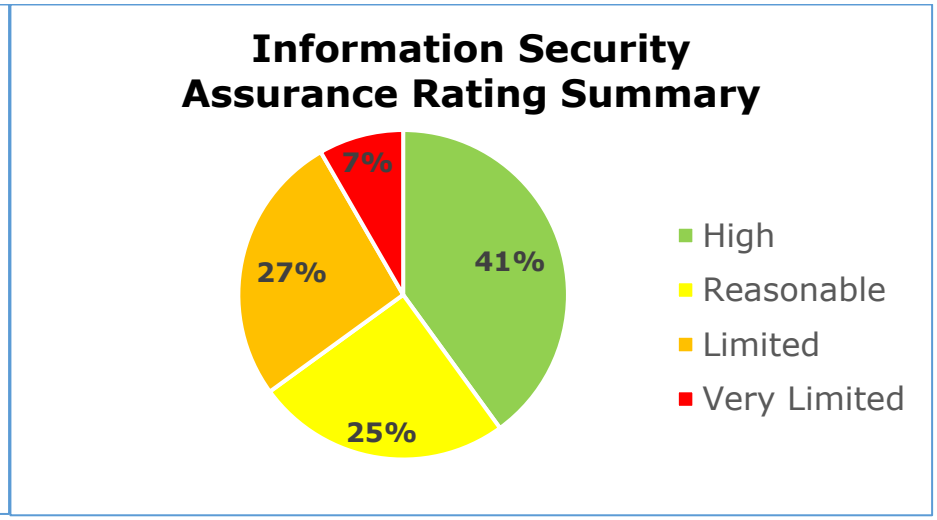
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

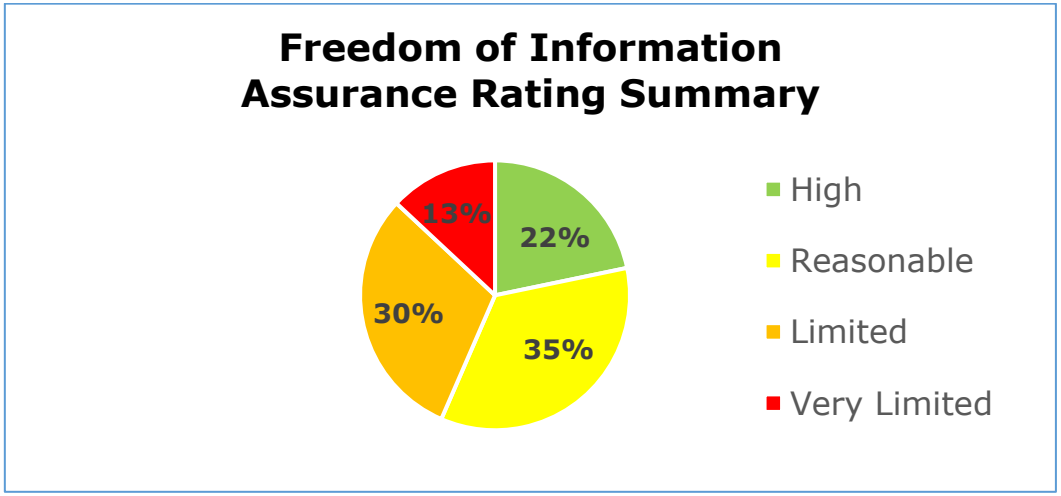
Priority Recommendations



Graphs and Charts







Areas for Improvement

- The DPO does not currently have sufficient oversight of all personal data being processed within GCC due to not sitting on all appropriate boards and groups that discuss personal data, and a lack of procedures ensuring the DPO is involved in all matters relating to the processing of personal data in a timely manner.

- GCC does not have a mandated Data Protection Impact Assessment (DPIA) policy in place outlining the procedure staff must follow when looking to undertake a new processing activity of personal data.

- GCC does not currently have a sufficient Record of Processing Activities (ROPA) document in place.

- A sufficient level of data protection training is not currently delivered to all staff on a routine basis.

- A number of active encrypted USB sticks are in use at GCC without identified ownership. As personal data could potentially be stored on these devices without oversight, this risks compromising effective information management.

- Disaster Recovery plans are not fully documented on a granular level and not all managed applications have been fully tested.

- There is a non-standardised way of promoting FOI through the council, particularly to new starters, and therefore a risk that not all new starters are provided with the level of information they should be.

- GCC are unable to meet statutory timescales for responding to FOI/EIR requests.

- There have been cases where information request responses are designed to meet the requirements of the Council rather than to meet legislation requirements.

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