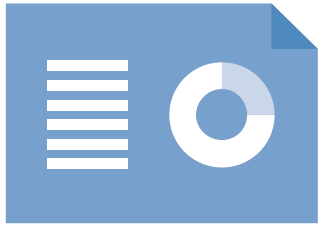
Torbay Council

Data protection audit report

November 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.

Torbay Council (TC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 16 September 2020 with representatives of TC to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and TC with an independent assurance of the extent to which TC, 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, TC agreed to the audit on a remote basis. A desk based review of selected policies and procedures was carried out in advance of the audit and remote telephone interviews were conducted from 10 November to 12 November 2020. The ICO would like to thank TC for its flexibility and commitment to the audit during difficult and challenging circumstances.

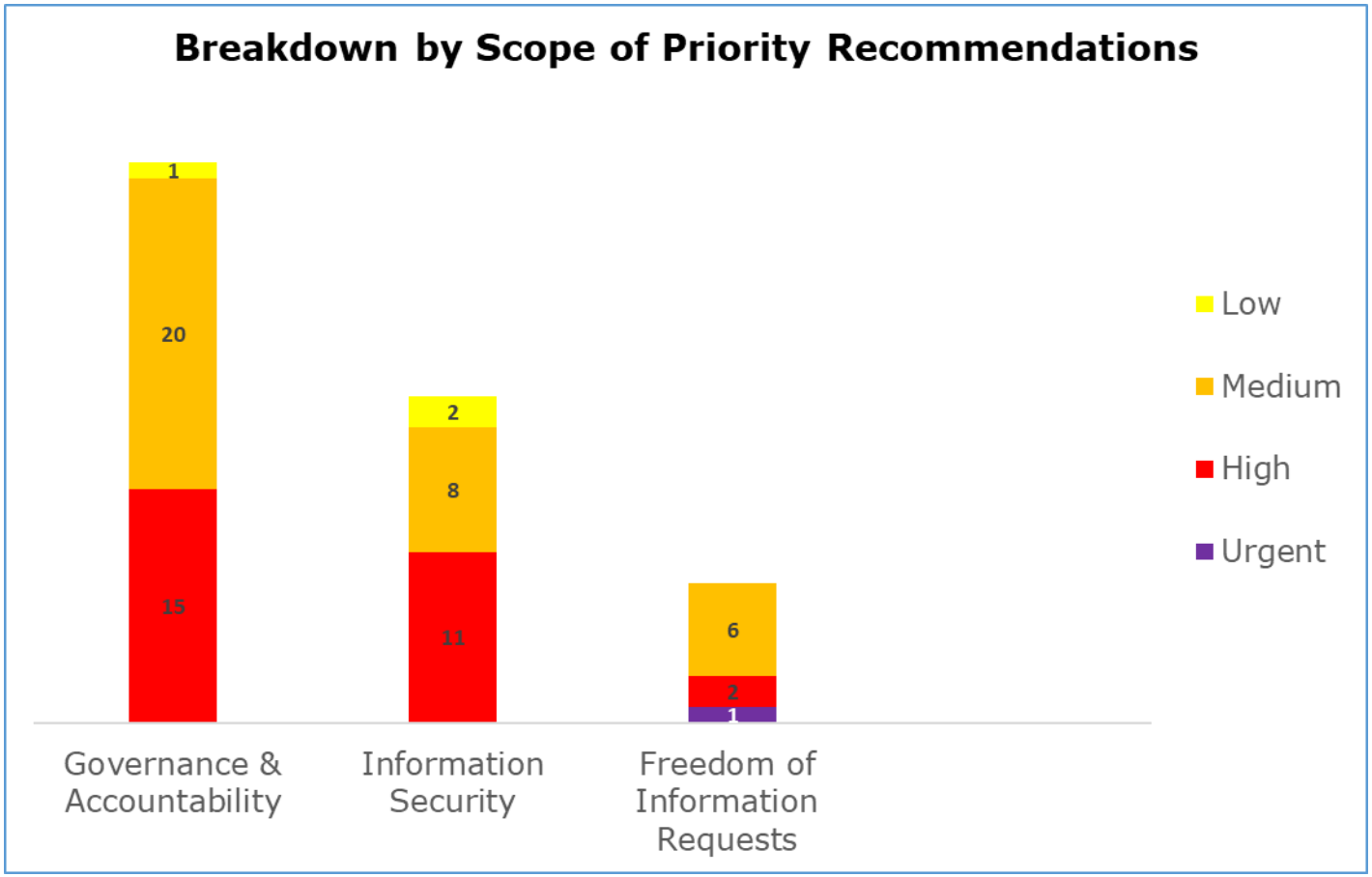
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist TC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. TC 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, FOI and EIR compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the relevant legislation.
Information Security	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection, FOI and EIR compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the relevant legislation.
Freedom of Information Requests	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection, FOI and EIR compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the relevant 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



Areas for Improvement

Set out a formal business plan outlining what resources are required to enable TC to effectively carryout its compliance obligations under the DPA 18 and GDPR.

Formally appoint one person who will hold the responsibilities for oversight for records management compliance across TC. These responsibilities should be documented in relevant policies and job description. Key performance indicators around records management should be set and reported against to the Information Governance Steering Group.

A record of processing activities should be documented for the processing TC undertakes when acting as a data processor for other controllers. This is a requirement under Article 30 of the GDPR.

Ensure that operating procedures are documented and are available in place. These should cover the work done by IT staff and to support its IT Infrastructure policy. By not having these procedures formally documented TC cannot demonstrate accountability as required by Article 5.2 of the GDPR.

The disaster recovery procedure is not sufficiently documented. A more detailed disaster recovery procedure should be created. This will enable TC to demonstrate the measures it has in place to prevent against the loss of personal data, as required by Article 5.1.f of the GDPR.

TC should conduct a review of their process for handling FOI requests to improve the response.

rates against statutory timeframes.

Best Practice

There is an electronic information asset register and ROPA management software in place.

The data protection officer sits on key project boards and advises on any planned processing of personal data.

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