Plymouth City Council

Data protection and freedom of information audit report

April 2024

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), as well as the Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIR). 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. Section 47 of the FOIA provides provision for the Commissioner to assess whether a public authority is following good practice, including compliance with the requirements of this Act and the provisions of the codes of practice under sections 45 and 46.

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 and freedom of information 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.

Plymouth City Council (PCC) agreed to a consensual audit of its data protection, freedom of information and environmental information regulations (EIR) practices.

The purpose of the audit is to provide the Information Commissioner and PCC with an independent assurance of the extent to which PCC, within the scope of this agreed audit, is complying with data protection legislation, the Freedom of Information Act (FOIA) and the Environmental Information Regulations (EIR).

The scope areas covered by this audit are determined following a risk based analysis of PCC's processing of personal data. The scope may take into account any data protection issues or risks which are specific to PCC's identified from ICO intelligence or PCC's own concerns, or any 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 PCC, the nature and extent of PCC's processing of personal data and handling of information requests, and to avoid duplication across scope areas. As such, the scope of this audit is unique to PCC.

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.
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.
Freedom of Information	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 public authority.

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

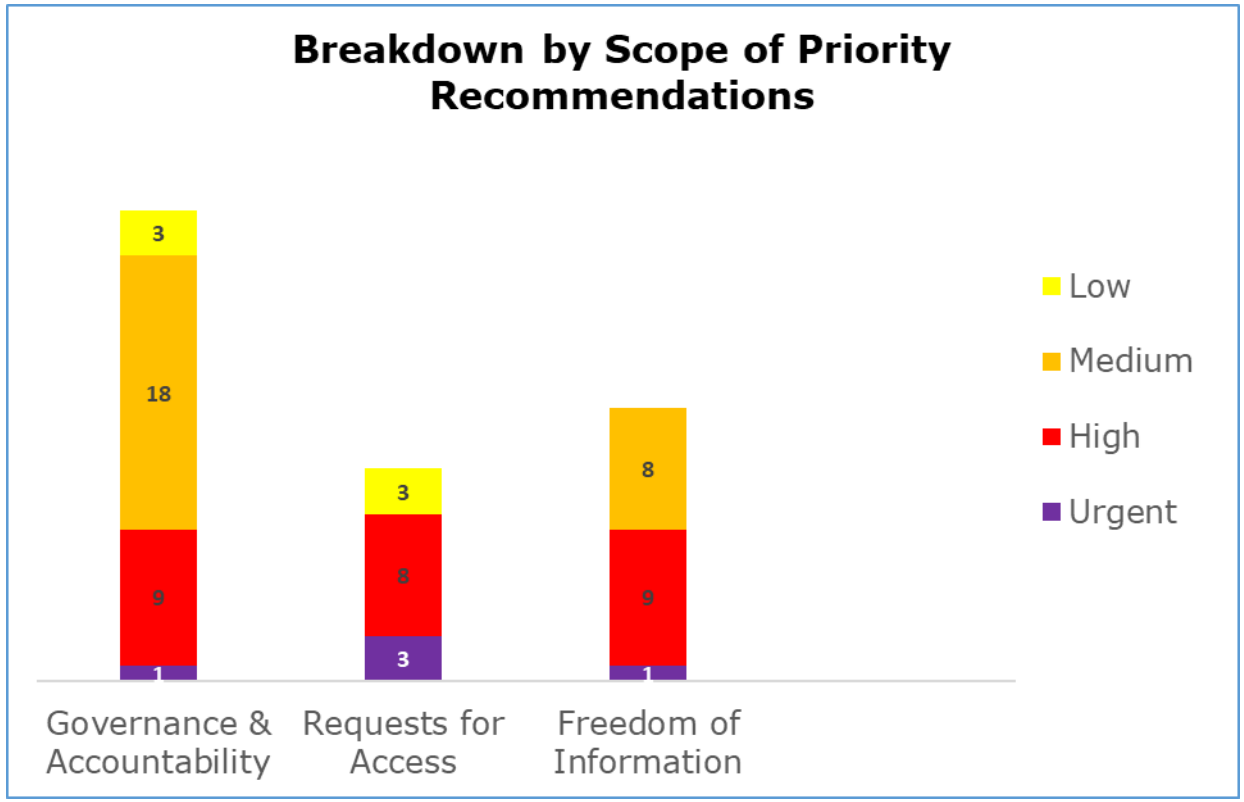
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist PCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they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

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.
Requests for Access	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.
Freedom of Information	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering compliance with the FOIA and EIR. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the legislation.

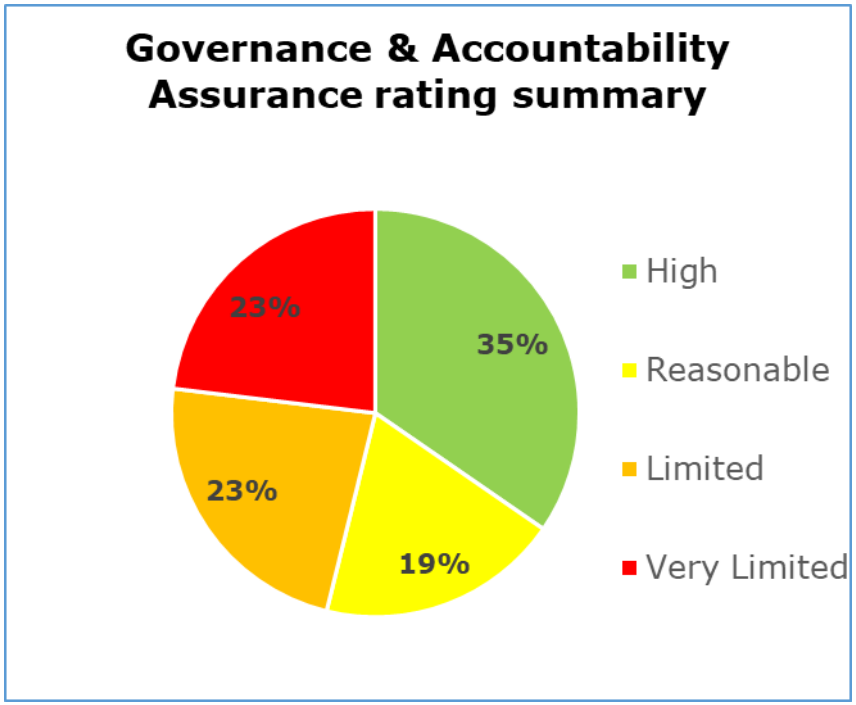
The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

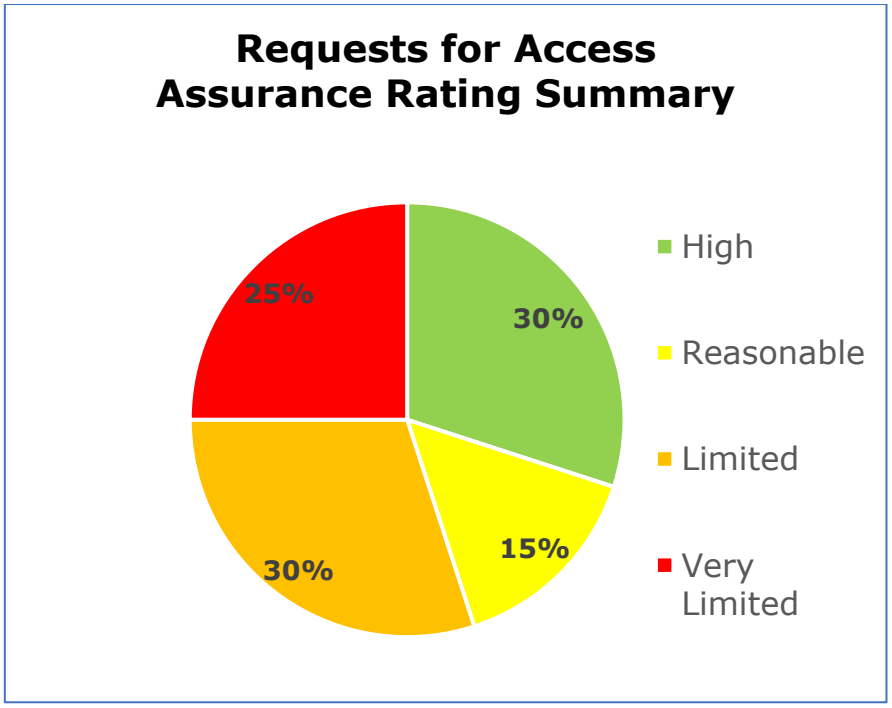


- Governance & Accountability has one urgent, nine high, 18 medium and three low priority recommendations.
- Requests for Access has three urgent, eight high, and three low priority recommendations.
- Freedom of Information has one urgent, nine high and eight medium priority recommendations.

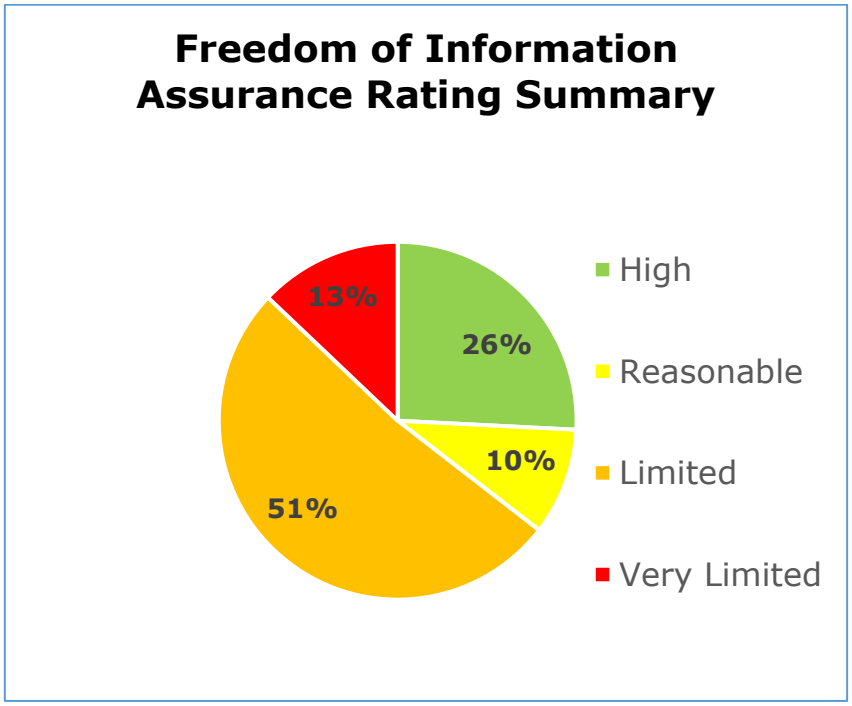
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 35% high assurance, 19% reasonable assurance, 23% limited assurance, 23% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 30% high assurance, 15% reasonable assurance, 30% limited assurance, 25% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 26% high assurance, 10% reasonable assurance, 51% limited assurance, 13% very limited assurance.

Areas for Improvement

Governance and Accountability

- PCC must undertake a fully comprehensive data mapping exercise to identify and understand what and how data flows into, around and out of the organisation.
- PCC should put in place Data Sharing Agreements (DSAs) with third parties as appropriate.
- PCC must ensure that all live processing of personal data has been underpinned by a Data Protection Impact Assessment (DPIA).
- PCC should undertake a Training Needs Analysis (TNA) to ensure that data protection training is aligned to the specific risks and responsibilities of each postholder and area.

Requests for Access

- PCC must continue with its considerations of ways to meet the workload of Subject Access Requests (SARs) more effectively, and ensure it has adequate resources in place to meet demand.
- PCC should review its use of extensions to information requests.
- PCC should provide all staff with sufficient training to be able to recognise a SAR in all forms, and know their role and responsibilities in handling SARs.
- PCC should put in place council-wide processes and procedures, setting out its approach to information requests and potential breaches of legislation.

Freedom of Information

- PCC should create a Freedom of Information (FOI) and Environmental Information Regulations (EIR) policy that explains the council's approach to and responsibilities for FOI and EIR.
- PCC must continue with its plans to improve FOI/EIR compliance across the council, to ensure compliance with statutory timescales.
- PCC should ensure that all staff with responsibility for responding to FOI/EIR requests receive specialised FOI/EIR training on an appropriate periodic basis.

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