Centrepoint

Data protection audit report

December 2022

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 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 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.

Centrepoint requested an audit from the ICO in June 2022 and submitted an audit questionnaire detailing the charity's data protection compliance concerns. ICO audit team managers completed a scoping call with Centrepoint to further discuss the charity's current data protection compliance levels and the appropriate scope areas on which to focus the audit.

The purpose of the audit is to provide the Information Commissioner and Centrepoint with an independent assurance of the extent to which Centrepoint, 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 Centrepoint's processing of personal data. The scope may take into account any data protection issues or risks which are specific to

Centrepoint, identified from ICO intelligence or Centrepoint'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 Centrepoint, the nature and extent of Centrepoint's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to Centrepoint.

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

Scope area	Description
Governance and 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.
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

Audits are conducted following the Information Commissioner's data protection 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.

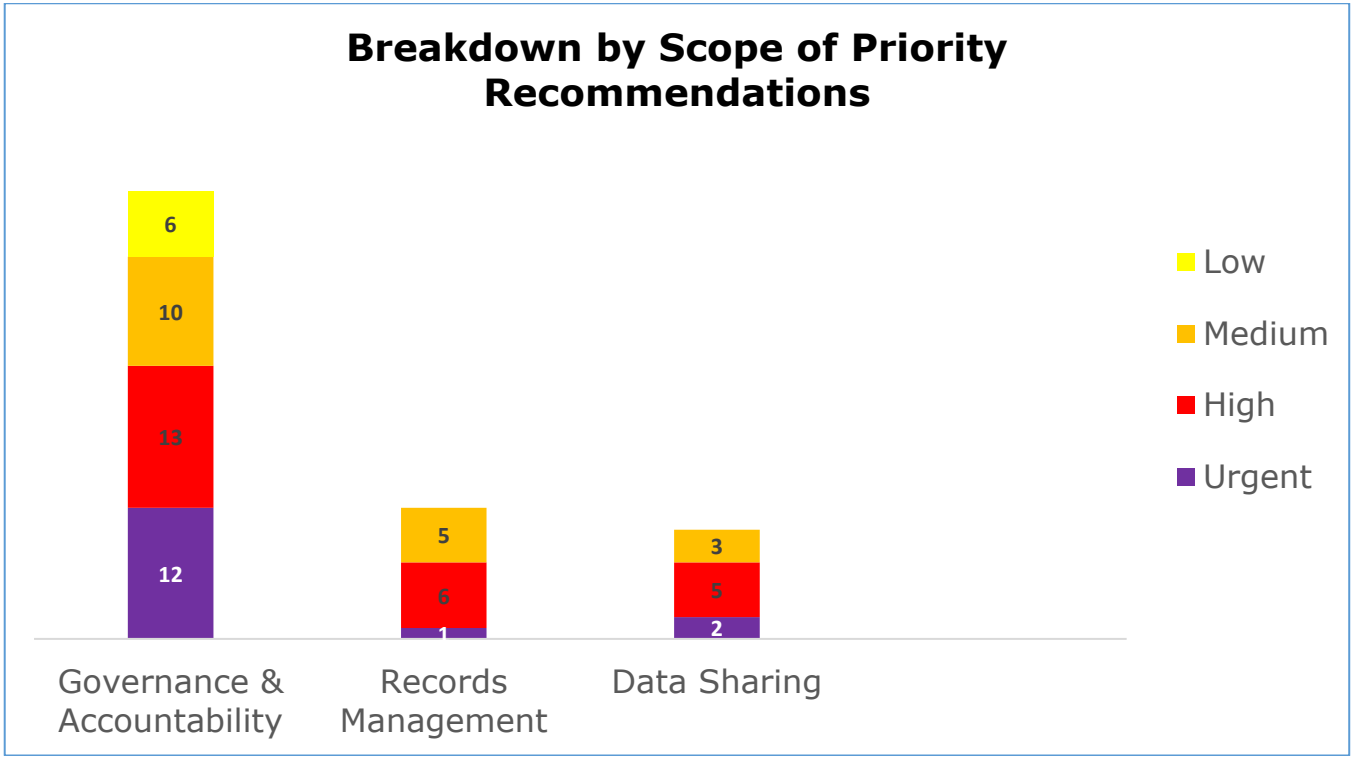
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist Centrepoint in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Centrepoint'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 and Accountability	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.
Records Management	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.
Data Sharing	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 and the rating may not necessarily represent a comprehensive assessment of compliance.

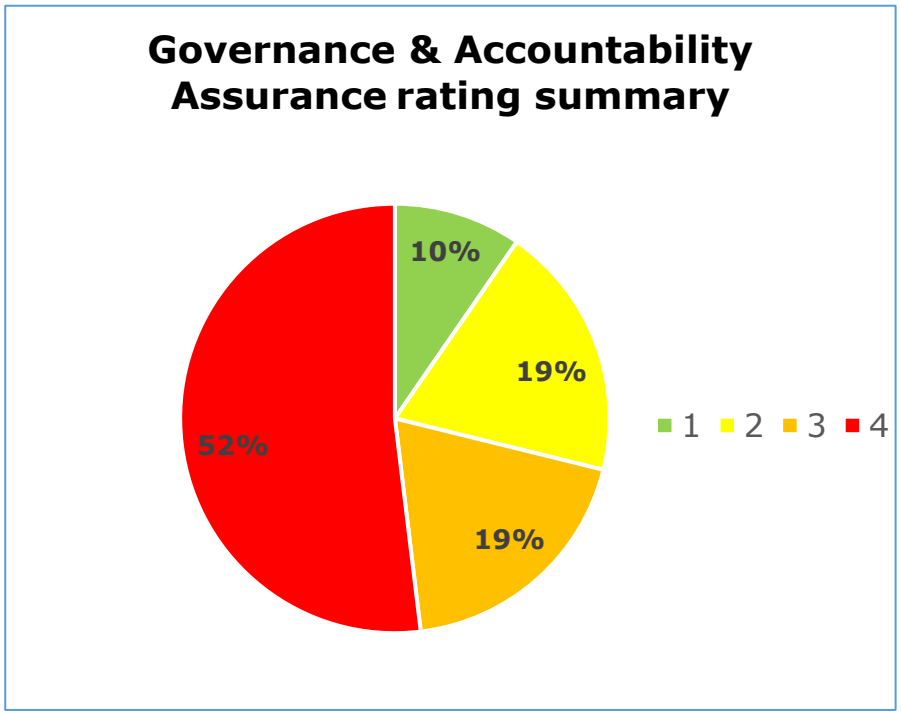
Priority Recommendations



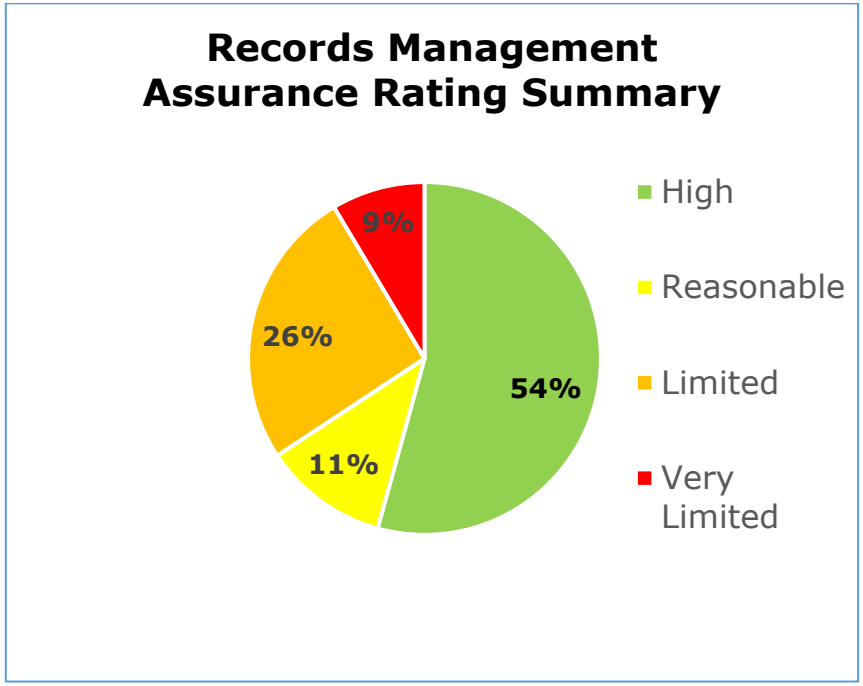
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 12 urgent, 13 high, 10 medium and six low priority recommendations
- Records Management has one urgent, six high and five medium priority recommendations
- Data Sharing has two urgent, five high and three medium priority recommendations

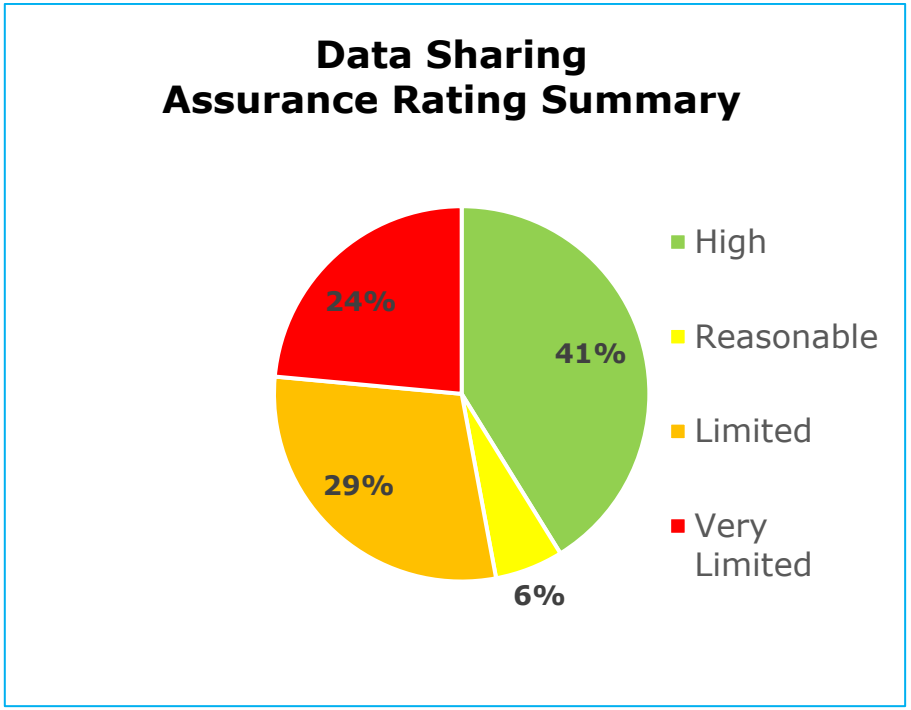
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 10% high assurance, 19% reasonable assurance, 19% limited assurance, 52% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 54% high assurance, 11% reasonable assurance, 26% limited assurance, 9% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 41% high assurance, 6% reasonable assurance, 29% limited assurance, 24% very limited assurance.

Areas for Improvement

Governance and Accountability:

Document the existing information management framework and expand it to include additional recommended roles which support the effective management of information, such as a Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs).

Develop a designated steering group, chaired by the DPO and attended by operational staff from across the organisation. This will provide an effective oversight of data protection and information governance within Centrepoint.

Roll out to all staff as planned the refresher training package recently purchased and carry out analysis to identify where staff in specific roles may require additional training, and to establish what this should include.

Amend existing data processor contracts and the data processor template to ensure that contracts always include thorough processing instructions, as required by UK GDPR Article 28(3).

As a precursor to the creation of a Record of Processing Activities (ROPA) produce data mapping exercises, set a deadline for document completion, and ensure all categories of data are captured.

Review the documented Lawful Bases for processing to ensure the most appropriate one for processing is used.

Review all current Data Protection Impact Assessments (DPIAs) as there is a lack of staff awareness on the need for them to be completed, monitored, and reviewed to mitigate any new or existing risks.

Records Management:

Appoint a Board member, who will have lead responsibility for the oversight of Records Management (RM). Include RM as an agenda item at meetings. This will ensure that Centrepoint has oversight and direction in place at a senior level for its RM function.

Create a RM policy which is subject to senior management approval, that undergoes periodic reviews and is communicated effectively to staff so that they are fully aware of the contents to ensure consistent practice across the charity.

Create a documented programme of data quality reviews across the charity that confirms information is still adequate for its original purposes and demonstrate evidence that the results of the reviews are acted on to refresh or improve information retention practices.

Data Sharing:

Create and review data sharing policies and procedures to ensure they are accurate and fit for purpose.

Complete a data sharing assessment and document the legality of data sharing in all relevant instances to ensure that Centrepoint can always be confident in the legality of its sharing decisions and can demonstrate why it is.

Following the completion of the data mapping exercise, Centrepoint must ensure they have an accurate and detailed Data Sharing Agreement (DSA) log, and that DSA and Data Processor Agreements are fit for purpose, or where absent, are established.

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 Centrepoint.

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