Cheshire Constabulary

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.

Cheshire Constabulary (CC) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 7 May 2021 with representatives of the CC to discuss the scope of the audit.

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

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

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 with Part 3 of the DPA18 and other national data protection legislation are in place and in operation throughout the organisation.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
Training and Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.

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, CC 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 26 to 28 July. The ICO would like to thank CC 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 CC 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. CC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

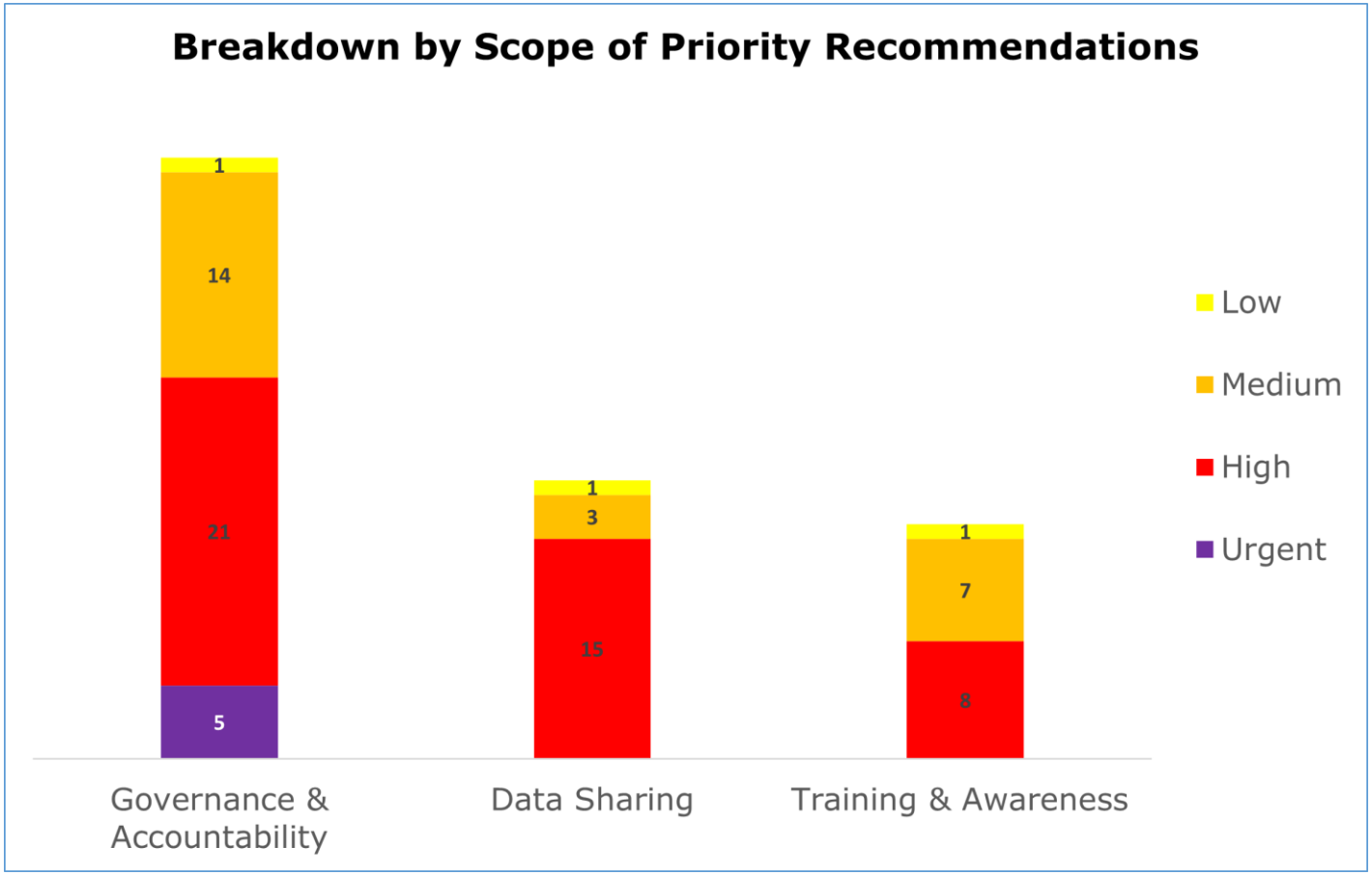
Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	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.
Training and awareness	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.

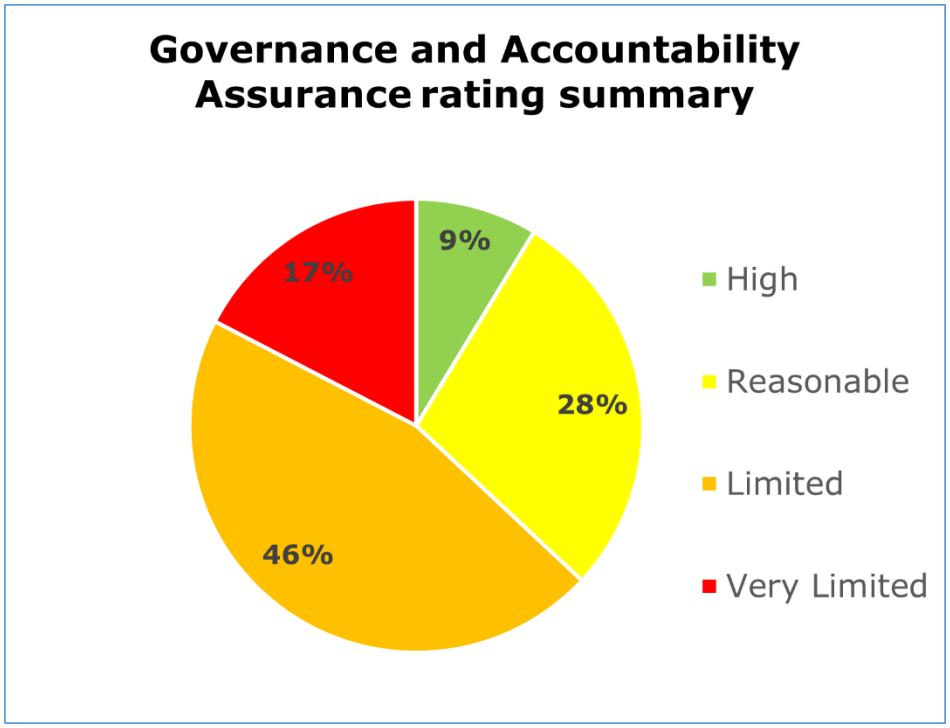


The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 5 urgent, 21 high, 14 medium and 1 low priority recommendations
- Data Sharing has 15 high, 3 medium and 1 low priority recommendations
- Training and Awareness has 8 high, 7 medium and 1 low priority recommendation

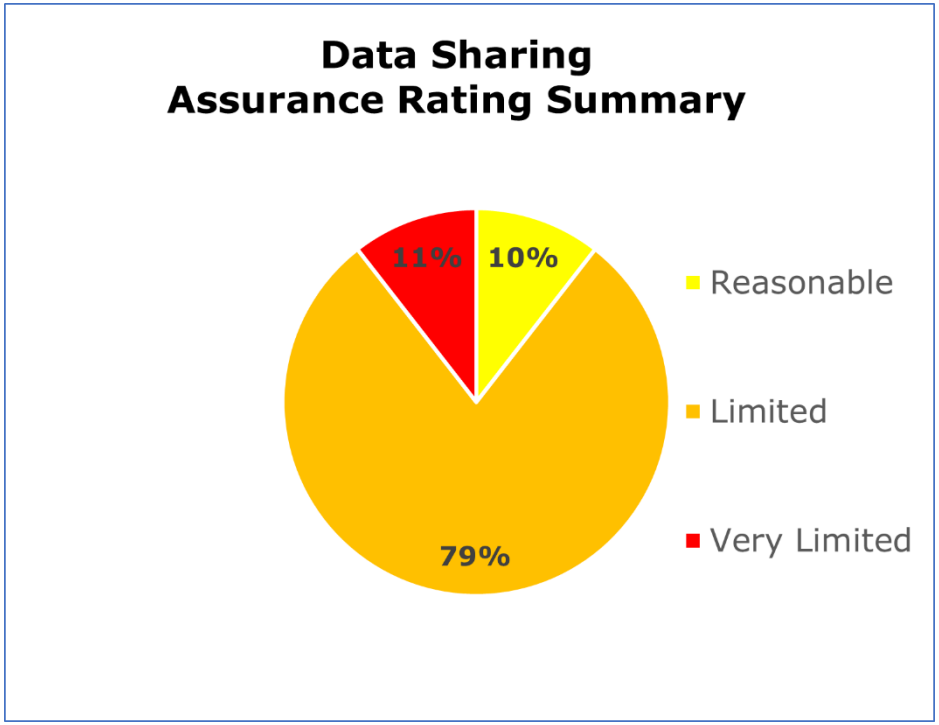
Graphs and Charts

A pie chart showing the percentage breakdown of the assurance ratings given for the Governance and Accountability scope.



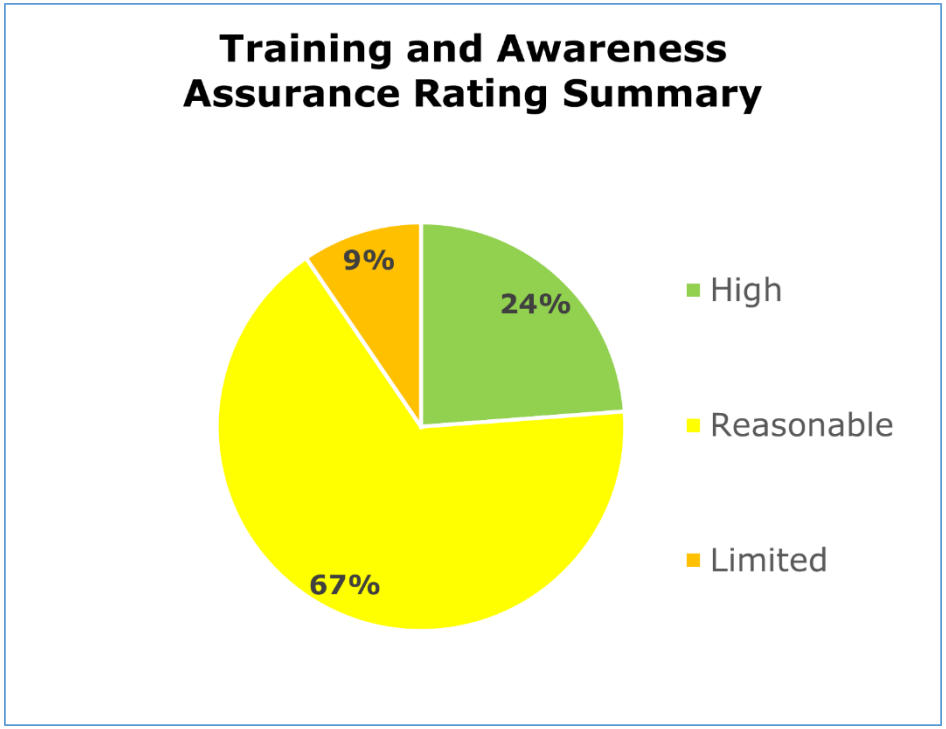
The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 9% high assurance, 28% reasonable assurance, 46% limited assurance, 17% very limited assurance.

A pie chart showing the percentage breakdown of the assurance ratings given for the Data Sharing scope.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 10% reasonable assurance, 79% limited assurance, 11% very limited assurance.

A pie chart showing the percentage breakdown of the assurance ratings given for the Training and Awareness scope.



The pie chart above shows a summary of the assurance ratings awarded in the Training and Awareness scope. 24% High assurance, 67% reasonable assurance, 9% limited assurance.

Areas for Improvement

- Not all tasks, as stipulated within section 71 of the DPA18 are appropriately assigned to the Data Protection Officer (DPO), such as data protection (DP) training and conducting audits. CC should review current resourcing within the Information Assurance Framework (IAF) to ensure the DPO has full capacity to complete tasks assigned to the role.

- A comprehensive data mapping exercise (information audit) has yet to be completed across all business areas. Therefore not all of the data processing that takes place across the constabulary is accounted for. This includes a lack of identification and oversight of all data processors and appropriate contracts.

- Review existing Records of Processing Activities (ROPA) to check that they are sufficiently granular. This will ensure accuracy of the ROPAs are maintained, that all relevant requirements of the legislation are documented and the most appropriate lawful basis for processing, including any sensitive processing, has been assigned. Key stakeholders within the organisation should assist in this process, such as Information Asset Owners (IAO's), Information Asset Assistants (IAA's) and Data Protection (DP) Champions.

- Revisit the use of consent as an appropriate lawful basis for law enforcement processing, including for the sharing of personal data, to establish whether consent in these instances is valid. It must be specific, require a positive opt-in and easy for data subjects to withdraw their consent. A process for recording and reviewing consent mechanisms must be established and formally documented.

- Review established data sharing activities to ensure there are appropriate Information Sharing Agreements (ISA's) in place. Confirm that sharing is aligned with the statutory requirements of the ICO Data Sharing Code of Practice. ISA's and associated Data Protection Impact Assessments (DPIAs) should be reviewed to

ensure they contain all the necessary detail, such as the established lawful basis for processing, the effectiveness of partners security measures and their retention and deletion processes.

- Strengthen the provision of specific DP training for specialist roles, such as IAO's and IAA's, staff with responsibilities for data sharing, DPIAs and with greater responsibilities for Information Governance (IG) and DP. Begin to proactively seek feedback from staff about the IG/DP training they have undertaken to gauge its effectiveness. Consider including knowledge checks as part of the process to ensure DP obligations have been understood.

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 Cheshire Constabulary.

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