Derby City Council

Data protection audit report

October 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) and other data protection legislation. 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.

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.

Derby City Council (Derby CC) agreed to a consensual audit of its data protection practices.

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

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.
Cyber Security	The extent to which the organisation has appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of personal data and protect information processing systems and facilities from cyber security threats.
Personal Data Breach Management & Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate.

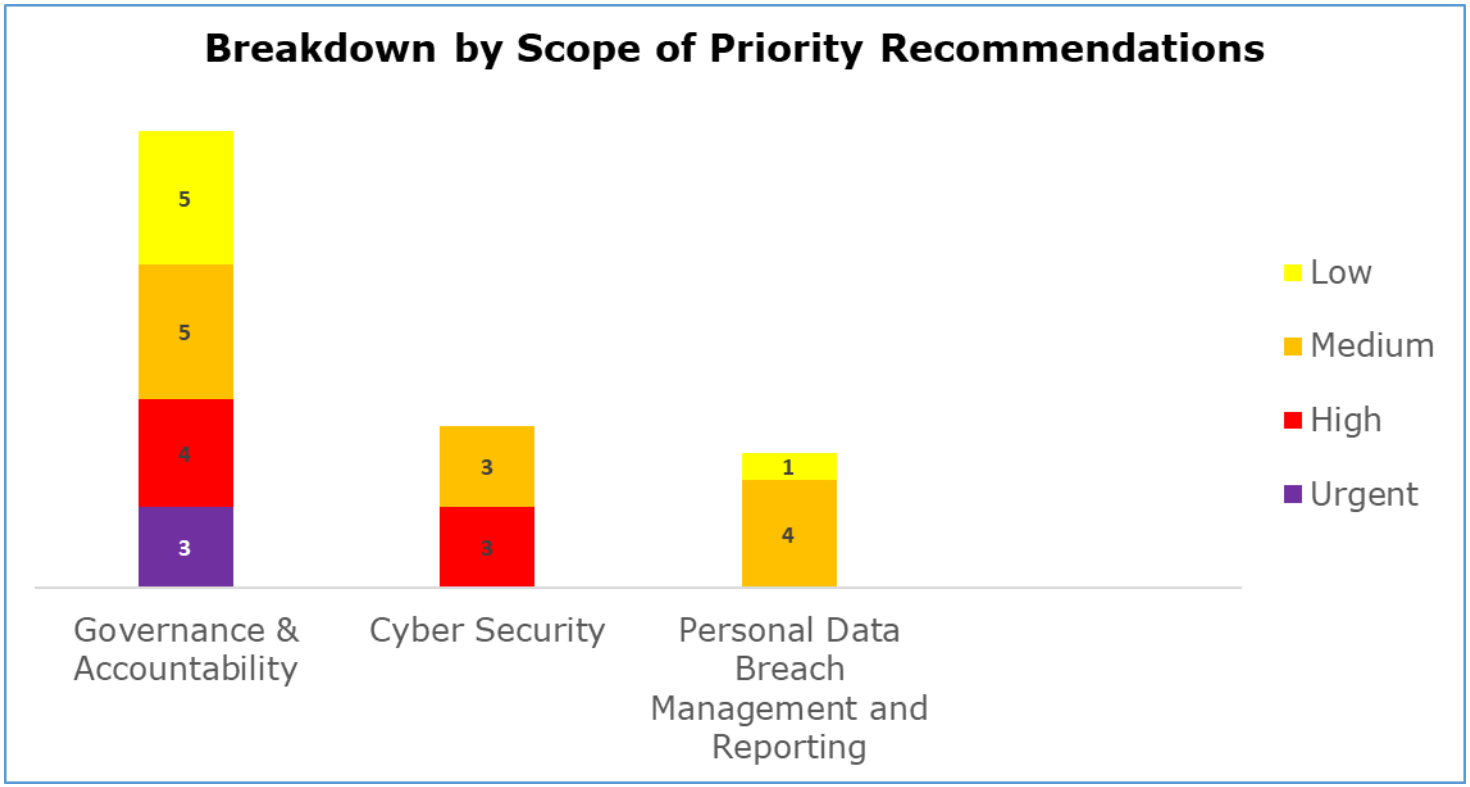
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential 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 Derby 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. Derby CC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

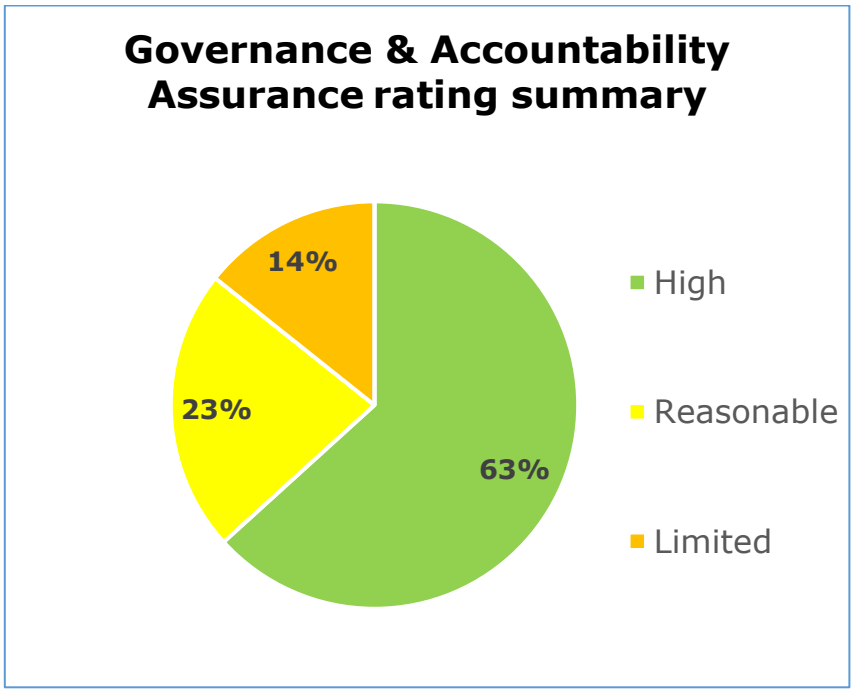
Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Cyber Security	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Personal Data Breach Management and Reporting	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

Priority Recommendations

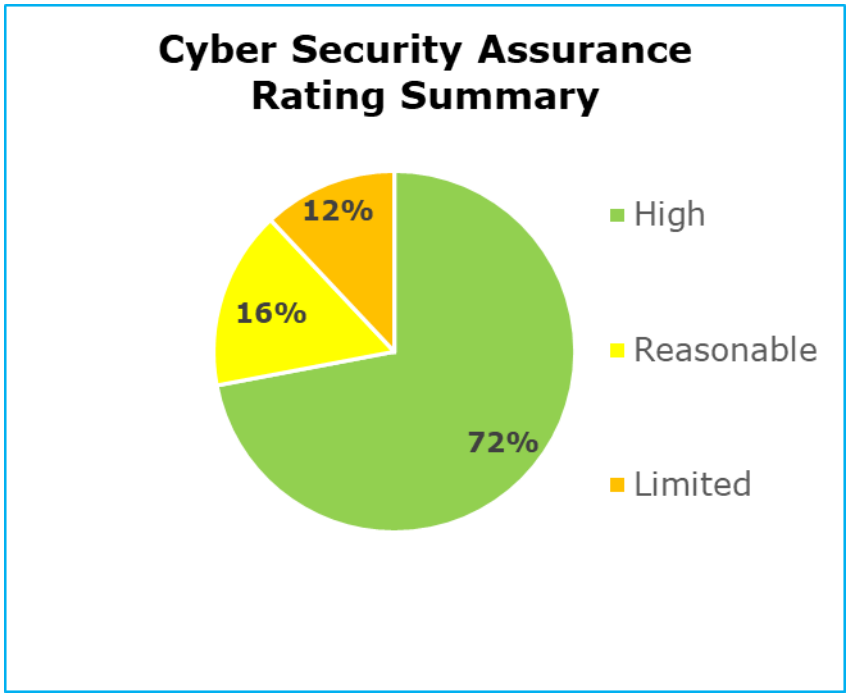


- Governance & Accountability has three urgent, four high, five medium and five low priority recommendations.
- Cyber Security has three high and three medium recommendations.
- Personal Data Breach Management and Reporting has four medium and one low priority recommendations.

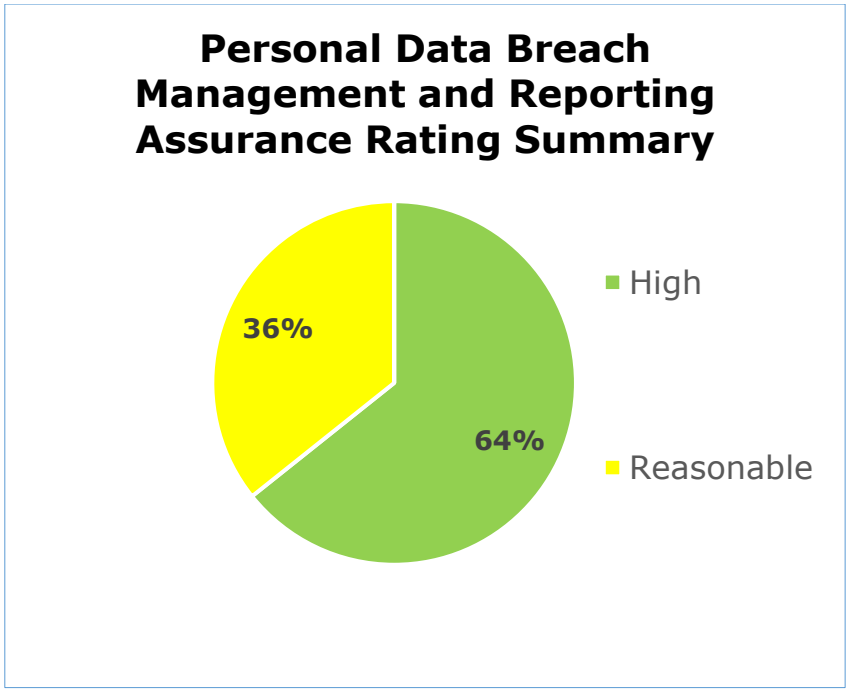
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. 63% high assurance, 23% reasonable assurance and 14% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Cyber Security scope. 72% high assurance, 16% reasonable assurance and 12% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management and Reporting scope. 64% high assurance and 36% reasonable assurance.

Areas for Improvement

Governance & Accountability

- Derby CC should complete a Training Needs Analysis (TNA) and ensure all roles receive specialist training that require it.
- Derby CC must ensure its Record of Processing Activities (ROPA) contains all required information, all entries are complete and are accurate, and based on information audits or data mapping, or both.
- Derby CC must ensure all high risk processing has a Data Protection Impact Assessment (DPIA) completed prior to processing taking place.

Cyber Security

- Derby CC should formalise its approach to Role Based Access Controls (RBAC), whereby user permissions are mapped and set up based on a pre-defined role profile.
- Derby CC should ensure that all cybersecurity-related policies are demonstrably reviewed or put forward to the relevant Board or Committee for approval, or both.

Personal Data Breach Management & Reporting

- Derby CC should ensure that staff with no access to a computer or Derby CC account, have access to policies, procedures and guidance that supports them in recognising and understanding how personal data breaches (PDBs) are handled.
- Derby CC should ensure that its retention schedule is reviewed regularly to guarantee that breach logs are always deleted in line with their retention period.

Best Practice

Governance & Accountability

- While Derby CC is not yet undertaking any automated decision making, there has been proactive work to ensure that it is already embedded in guidance and privacy notice templates.
- Derby CC has demonstrated a strong communication structure with IG being communicated through multiple channels with effective messaging. This has led to a strong privacy culture, as demonstrated through staff engagement in drop in sessions and the volume of queries received by the IG team.

Cyber Security

- Derby CC has run regular, varied and targeted phishing simulation campaigns since 2019. Where appropriate, subsequent tailored support and follow up training is given to users.

Personal Data Breach Management & Reporting

- Derby CC have templates in place that can be used to notify individuals of a PDB where appropriate. Derby CC always considers the method of communication before notifying an individual, considering factors such as the individual's age and vulnerability to determine the best method of notification. It was reported during interviews that Derby CC staff have conducted home visits to inform vulnerable individuals of a PDB. This gave them the opportunity to provide them with support and guidance on how to protect their personal data after a PDB has occurred.

Key areas of Assurance

Governance & Accountability

- Derby CC have strong compliance measures for mandatory training, locking staff out of accounts if not completed in a timely manner.
- Derby CC displayed a strong understanding and comprehensive guidance about UK GDPR Article 6 lawful bases and how they apply.
- Derby CC showed thorough processes and considerations made in the DPIA process, giving time and thought to all possible risks they can foresee.

Cyber Security

- Derby CC has embedded a governance structure which supports effective cyber security and IT change management.
- Derby CC has put in place appropriate measures to control and manage the allocation and use of privileged access rights.
- Derby CC demonstrated a proactive approach to patch and vulnerability management.
- Derby CC makes effective use of authentication methods.

Personal Data Breach Management & Reporting

- Derby CC have allocated appropriate responsibility for assessing, recording and reporting personal data breaches.
- Derby CC regularly review reported PDBs to identify trends, in order to provide additional support and guidance to areas of the council where there is an increase of PDBs.

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