Humberside Police

Data protection audit report

May 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.

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

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.
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

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, HP 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 April 2022 to 28 April 2022 the ICO would like to thank HP 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 HP 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. HP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

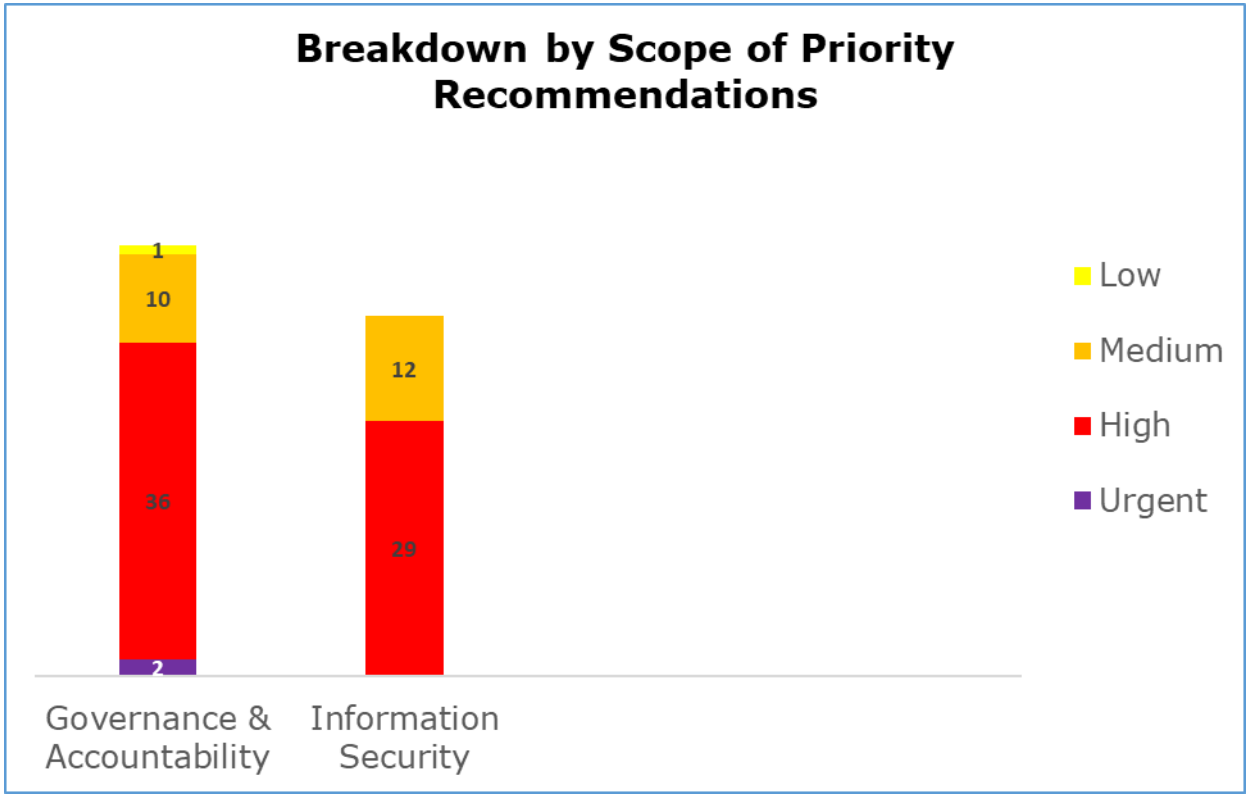
Audit Summary

Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	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.
Information Security	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.

*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.

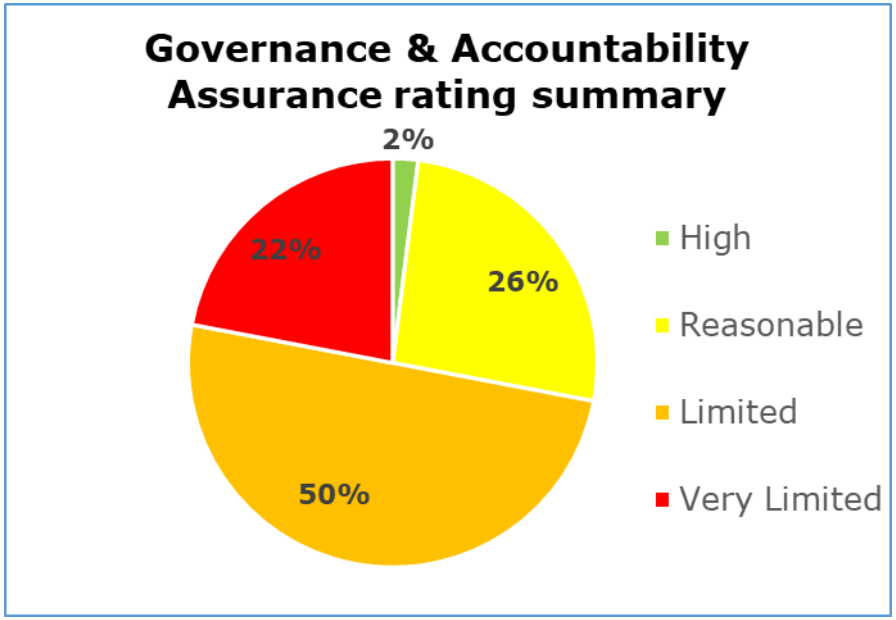


The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- The Governance and Accountability scope has 2 urgent, 35 high, 10 medium and 1 low priority recommendations
- The Information Security scope has 28 high, 12 medium priority recommendations

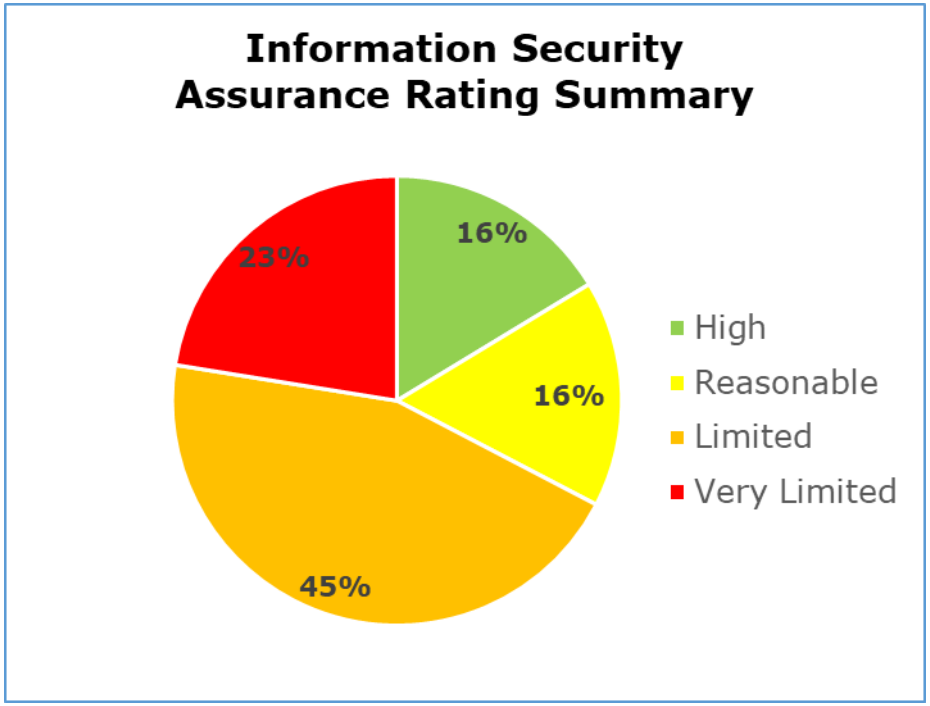
Graphs and Charts

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. 2% high assurance, 26% reasonable assurance, 50% limited assurance, 22% very limited assurance.

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 Information Security scope. 16% high assurance, 16% reasonable assurance, 45% limited assurance, 23% very limited assurance.

Areas for Improvement

Ensure HP have a sufficient dedicated resource from their data protections officer (DPO) and there is sufficient resource in place to support the day to day management of all aspects of IG and data protection.

Review and Update Information Governance (IG) policies and procedural guidance, including a Data Protection (DP) policy and Records Management (RM) policy that outline HPs approach to DP, Information Security (IS) personal data breaches (PDBs) and data sharing.

Review the Appropriate Policy Document (APD) to include HPs procedures for complying with the DP principles in its processing of personal data under Part 3 of the DPA18.

Develop and document an IG training programme instigated by a Training Needs Analysis (TNA) for all staff. The training should be regularly refreshed and include a programme of specialist training for IG and IS roles.

Review all contracts with data processors to ensure there is a process for reporting and responding to a Personal Data Breach (PDB).

Complete HP's information audit/data mapping exercise to incorporate all business areas across the force. The information audit/data mapping should inform HP's Record of Processing (ROPA)/Information Asset Register (IAR) to comply with Article 30 UKGDPR and s.61 DPA18 legislation. The ROPA/IAR should fully record the lawful basis for processing personal data including special category and sensitive processing of data.

A programme of risk-based IG audits should be developed to include areas of IG such as Records Management, Personal Data Breaches as well as Information Security as part of an internal audit plan. The programme of audits can support monitoring of staff compliance with DP policies and procedures.

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 Humberside Police.

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