Merseyside Police

Data protection audit report

August 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.

Merseyside Police (MP) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 14 April 2021 with representatives of MP to discuss the scope of the audit.

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

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.
Records Management	The extent to which processes are 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.
Personal Data Breach Management and 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 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 MP agreed to continue with the audit on a remote basis. A pre-audit survey was drafted by ICO Auditors and agreed by MP and launched to MP staff between 28 May and closed on 28 June. The ICO would like to thank MP 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 MP 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. MPs priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

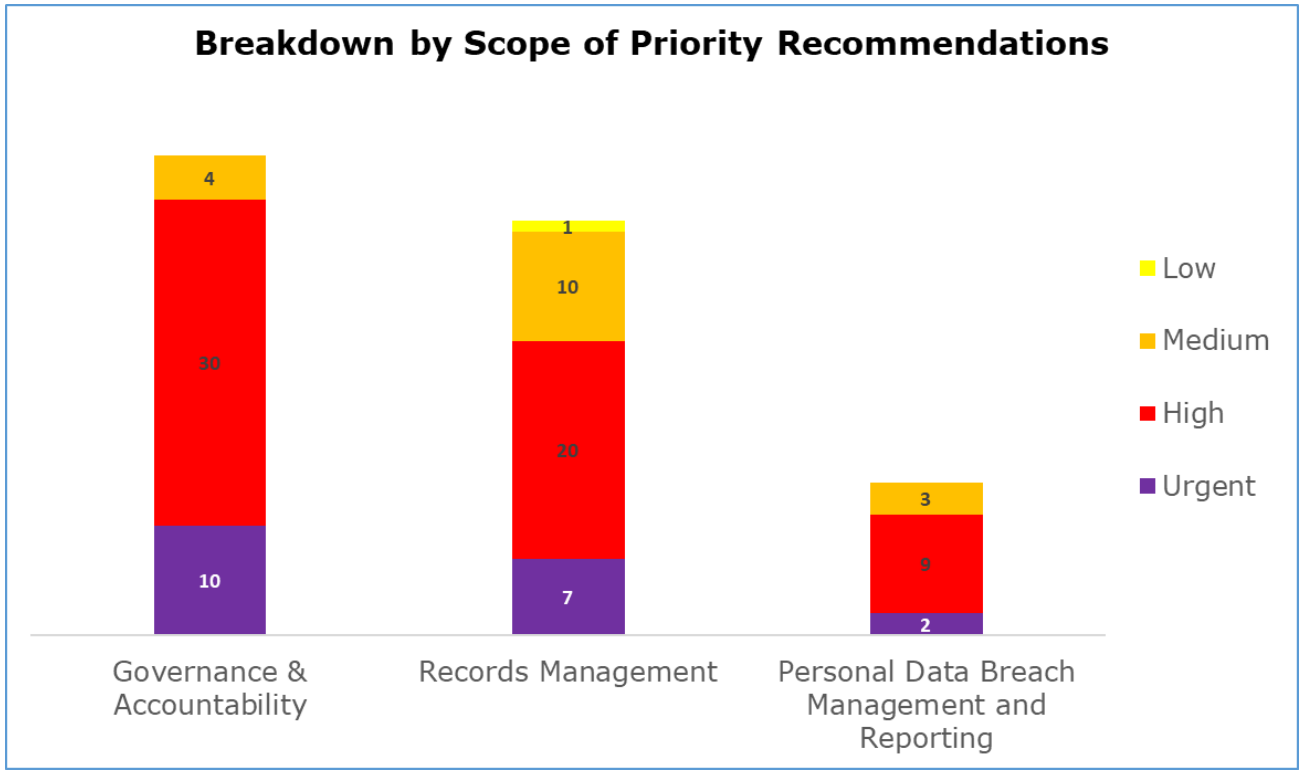
Appendix Two contains the results of the pre-audit survey. MP should use the results of the survey to inform their Information Governance (IG) training and awareness programme.

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	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.
Personal Data Breach Management and Reporting	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.

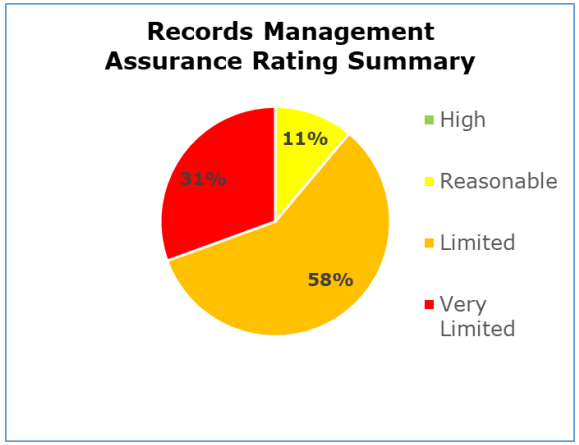
Priority Recommendations



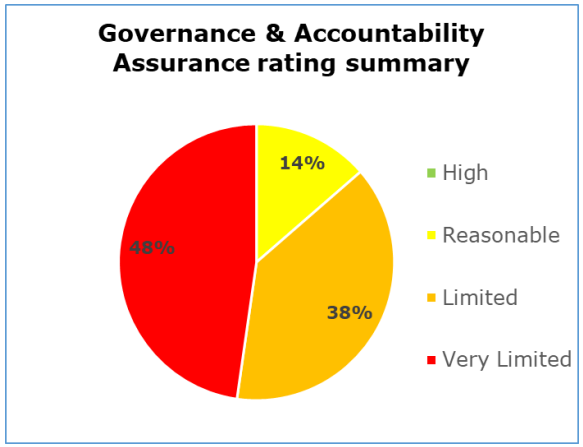
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has ten urgent, 30 high and four medium priority recommendations.
- Records Management has seven urgent, 20 high, ten medium and one low priority recommendations.
- Personal Data Breach Management and Reporting has two urgent, nine high, three medium priority recommendations.

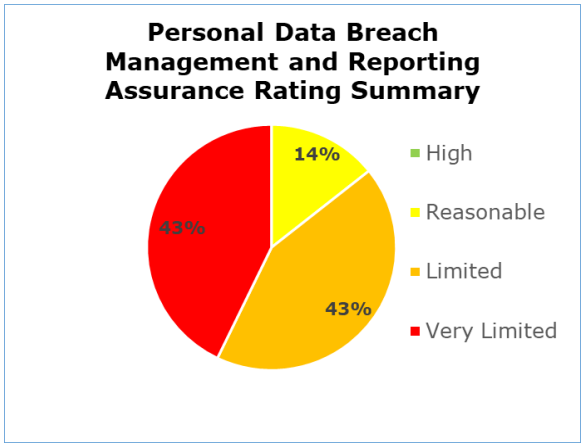
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 11% reasonable assurance, 58% limited assurance, 31% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 14% reasonable assurance, 38% limited assurance, 48% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management and Reporting scope. 14% reasonable assurance, 43% limited assurance, 43% very limited assurance.

Areas for Improvement

Develop a suite of key IG policies and practical procedural guidance, including a Data Protection (DP) policy and Records Management (RM) policy that outline MPs approach to DP, Information Security (IS), PDBs and data sharing. Producing guidance for individuals and staff would assist in handling requests for rectification and erasure of personal data. It will also help MP inform third parties to which that data was shared.

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

Design 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 roles.

Review all contracts with third party organisations who process personal information on behalf of MP to identify MPs data processors. Where a processor is used, an appropriate contract should be put in place that includes arrangements for reporting and responding to a PDB.

The completion of an information audit/data mapping exercise would ensure that all data processors are clearly identified and create both a complete Record of Processing Activities (RoPA) and Information Asset Register (IAR), to incorporate all business areas across MP. The exercise is key to comply with Article 30 UK GDPR and s.61 DPA18 legislation and establishing the lawful basis for processing personal data, special categories and sensitive processing of data.

To ensure that manual and electronic records containing personal data are appropriately accessed, classified, stored, weeded and disposed of, MP should document formal RM policies and procedures including sharing personal data with third parties across all areas of MP.

Tightening procedures around staff transferring roles within MP will assist with access control and ensuring staff only have access to systems and areas containing personal data that they are authorised to.

Identify and document a set criteria for assessing the severity of PDB and the likely effect on individual's rights and freedoms. This guidance should reference risk assessment guidance and provide particular information on how to assess a 'high risk' to affected individuals.

MP should develop a process and guidance for staff to follow when notifying individuals of a PDB. For law enforcement processing, where the provision of information about the breach is restricted wholly or partly, the procedure should ensure that the restriction is applied appropriately and consistently with the decision to restrict the provision of the information documented.

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