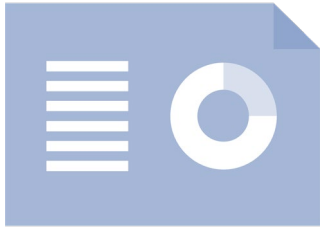
Metropolitan Police Service

Data protection audit report

November 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.

The Metropolitan Police Service (MPS) agreed to a consensual audit of it's processing of personal data. An introductory telephone meeting was held on 22 July 2021 with representatives of MPS to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and MPS with an independent assurance of the extent to which MPS, 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 MPS, 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 MPS, 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 MPS.

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.
Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the organisation.

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 MPS 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 4 to 11 October. The ICO would like to thank MPS for its flexibility and commitment to the audit during difficult and challenging circumstances.

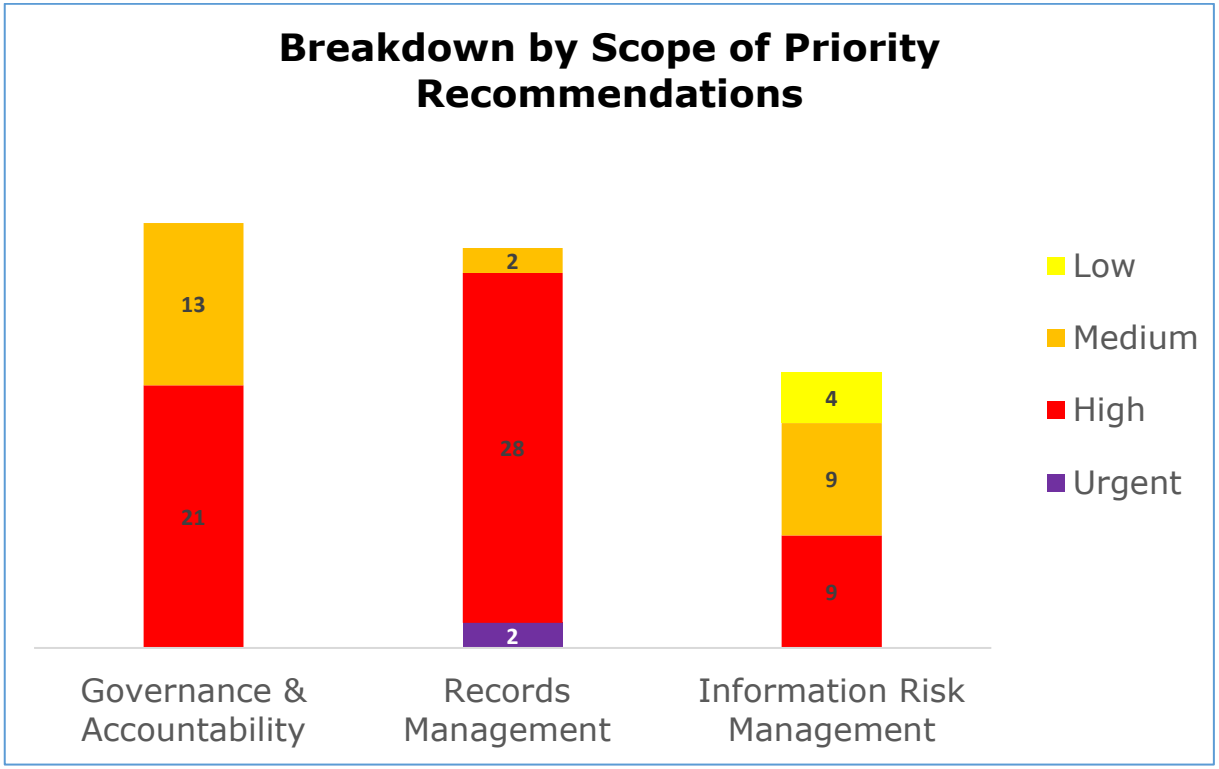
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist MPS in implementing the recommendations each has been assigned a priority rating based upon the risks that they 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.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and 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.
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.
Information Risk 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.

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.

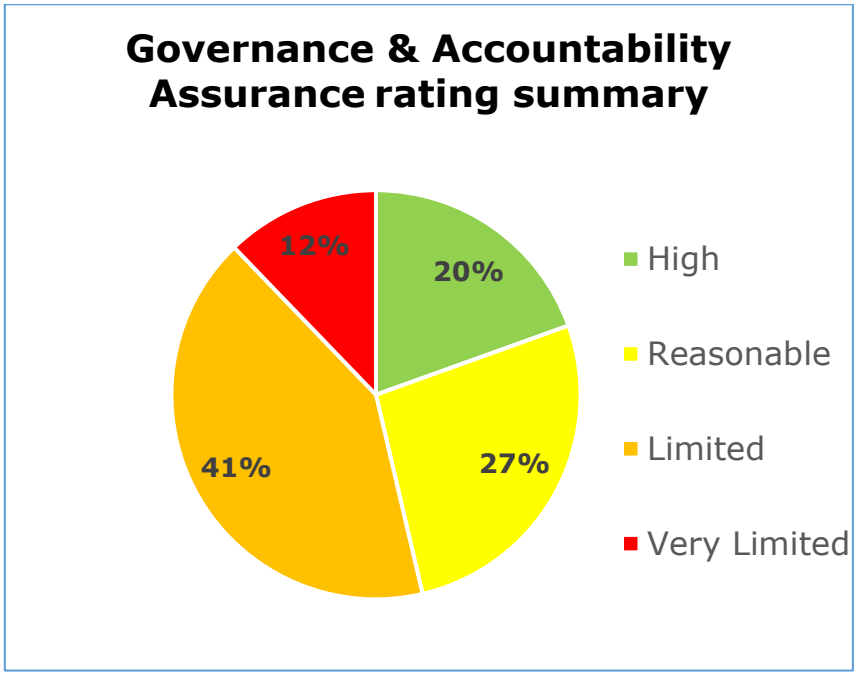
Priority Recommendations



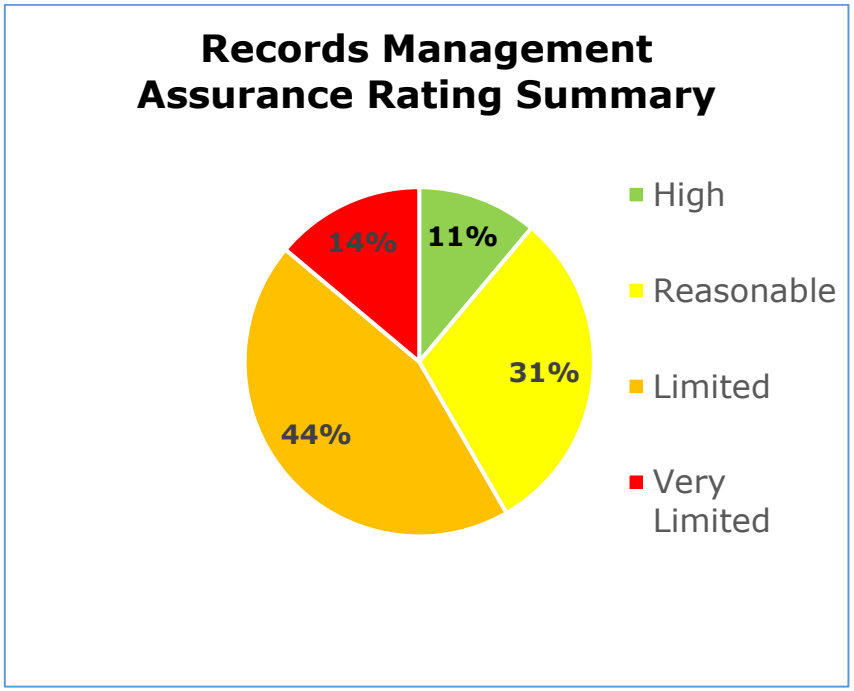
The bar chart above shows a breakdown by scope area of the priorities assigned to the recommendations made:

- Governance and accountability has 21 high and 13 medium priority recommendations
- Records Management has 2 urgent, 28 high and 2 medium priority recommendations
- Information Risk has 9 high, 9 medium and 4 low priority recommendations

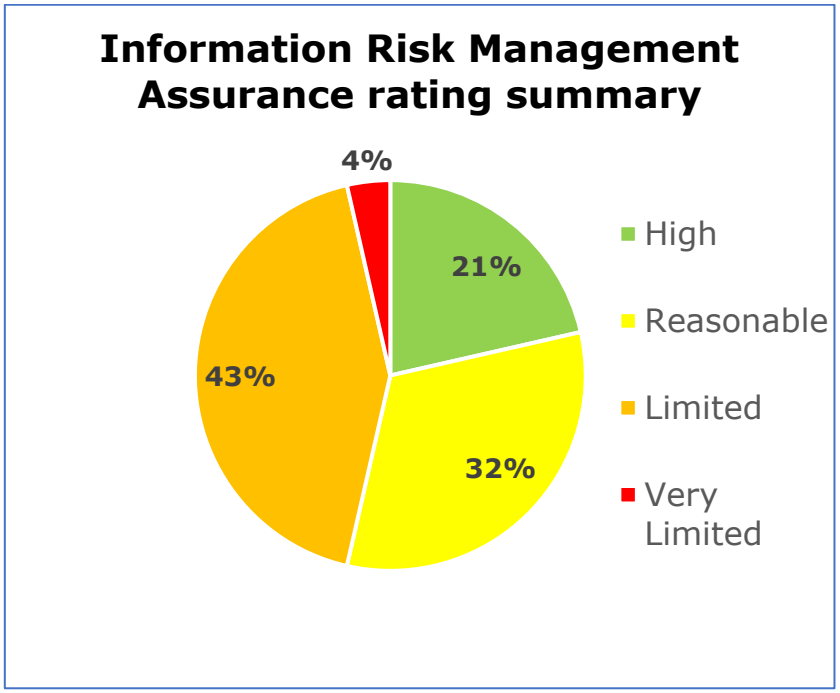
Graphs and Charts



A pie chart showing the percentage breakdown of the assurance ratings given for the Governance and Accountability scope.
20% high assurance, 27% reasonable assurance, 41% limited assurance, 12% very limited assurance.



A pie chart showing the percentage breakdown of the assurance ratings given for the Records Management scope. 11% high assurance, 31% reasonable assurance, 44% limited assurance, 14% very limited assurance.



A pie chart showing the percentage breakdown of the assurance ratings given for the Information Risk Management scope.
21% high assurance, 32% reasonable assurance, 43% limited assurance, 4% very limited assurance.

Areas for Improvement

The completion of an information audit (data mapping) across the whole organisation will ensure that all information assets have been identified and recorded. This will assist MPS in the completion of their Information Asset Register (IAR)/Record of Processing Activities (ROPA).

Continue to develop the IAR/ROPA to ensure compliance with Article 30 of the UKGDPR and Section 61 of the DPA18. A completed IAR/ROPA will assist MPS in ensuring the most appropriate lawful basis for processing and/or condition for sensitive processing has been chosen and will also help to identify and manage their information risks.

Continue to develop the Information Asset Owner (IAO) and Information Asset Assistant (IAA) role, ensuring that IAO's are assigned to all information assets. Ensure the IAO Handbook includes guidance on the risk management of information assets.

The completion of a Learning Needs Analysis (LNA) will strengthen the data protection (DP) training programme. The LNA should highlight any specialised training requirements outside of the Data Office (DO) that have DP responsibilities, including staff working in Records Management (RM), Data Protection Impact Assessments (DPIA), data sharing (DS) and front line/operational staff whose role includes the collection of personal data.

Continue to review the backlog of Management of Police Information (MOPI) graded files to ensure physical records containing personal data are not being retained for longer than they should. Establishing a procedure to ensure physical records are disposed of once an electronic record is deleted will assist MPS in adherence to their retention schedule.

Review all IT systems which process personal data for a law enforcement purpose to ensure MPS can meet all elements of the section 62 of the DPA18 requirements. Ensure the various ways in which the logs can be obtained are documented within a formal policy and/or procedure.

Formally documenting the process for reviewing DPIAs will ensure any changes to a project that involves the processing of personal data will be accounted for. The process should include what information staff are required to record.

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 the Metropolitan Police Service.

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