Independent Office for Police Conduct

Data protection audit report

July 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 Independent Office for Police Conduct (IOPC) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 3 March 2021 with representatives of the IOPC to discuss the scope of the audit.

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

It was agreed that the audit would focus on the following areas:

Scope area	Description
Records Management	The processes 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.
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 the IOPC 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 11 to 14 May 2021. The ICO would like to thank the IOPC for its flexibility and commitment to the audit during difficult and challenging circumstances.

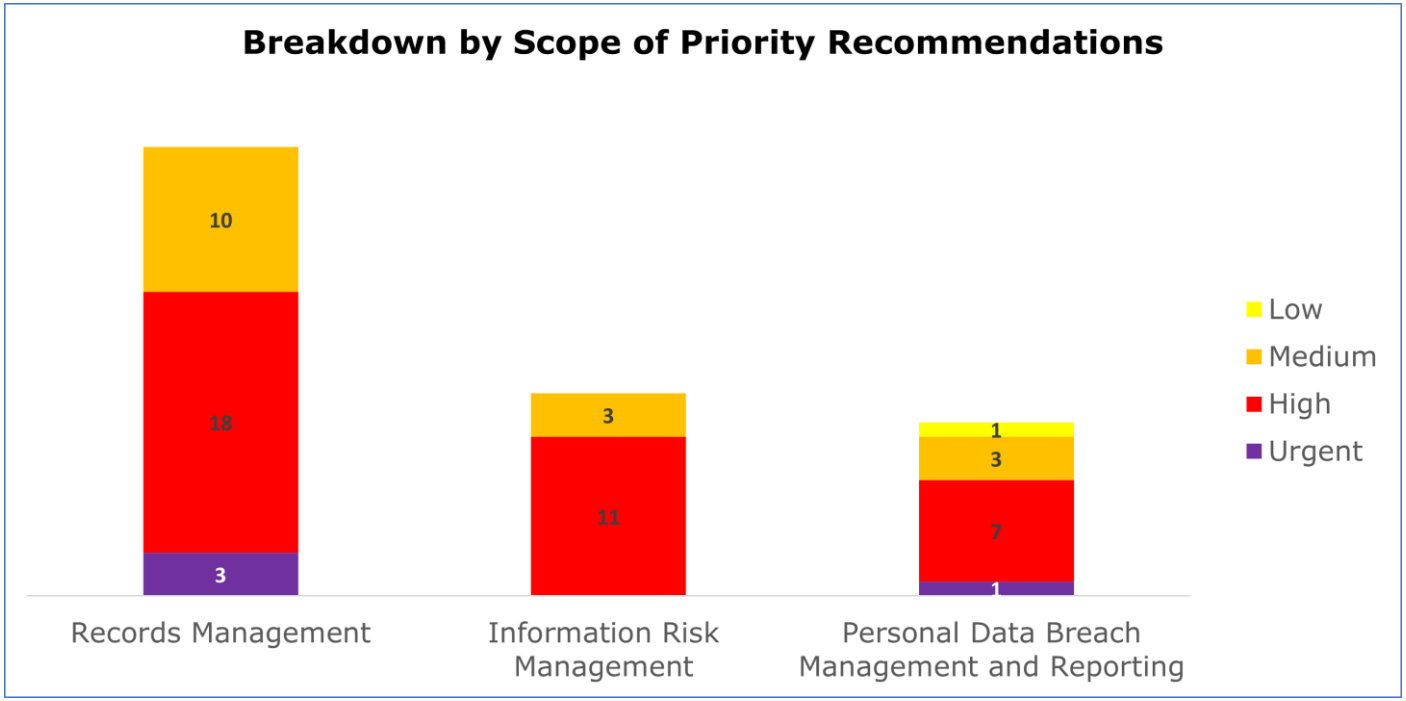
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the IOPC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The IOPC'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
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.
Personal Data Breach Management and Reporting	**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.

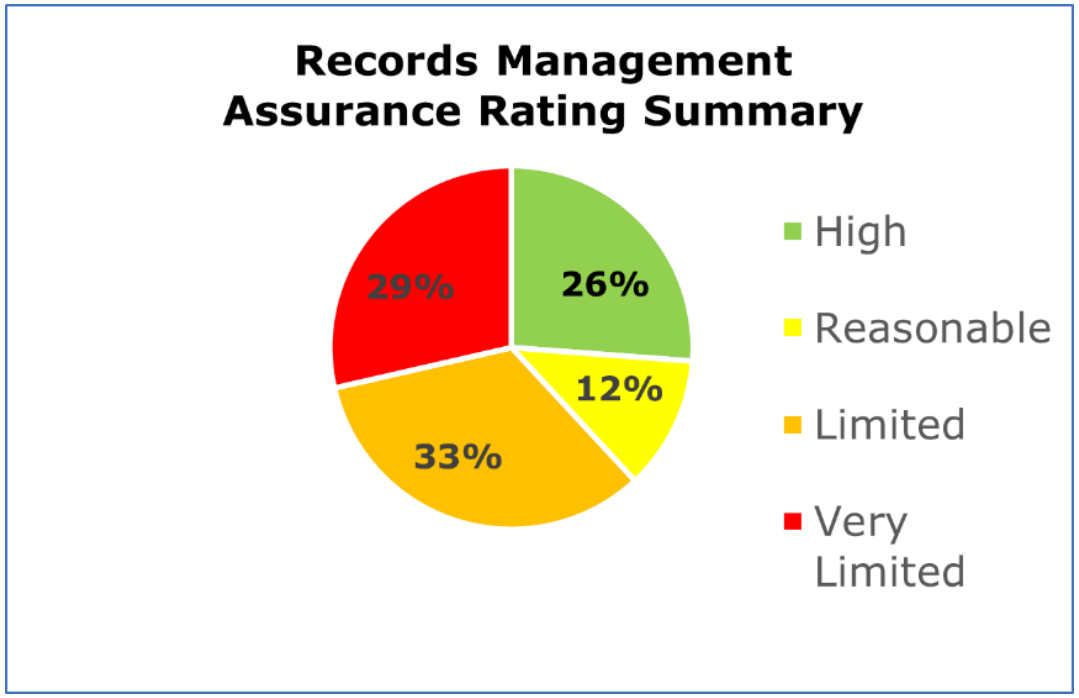
Priority Recommendations



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

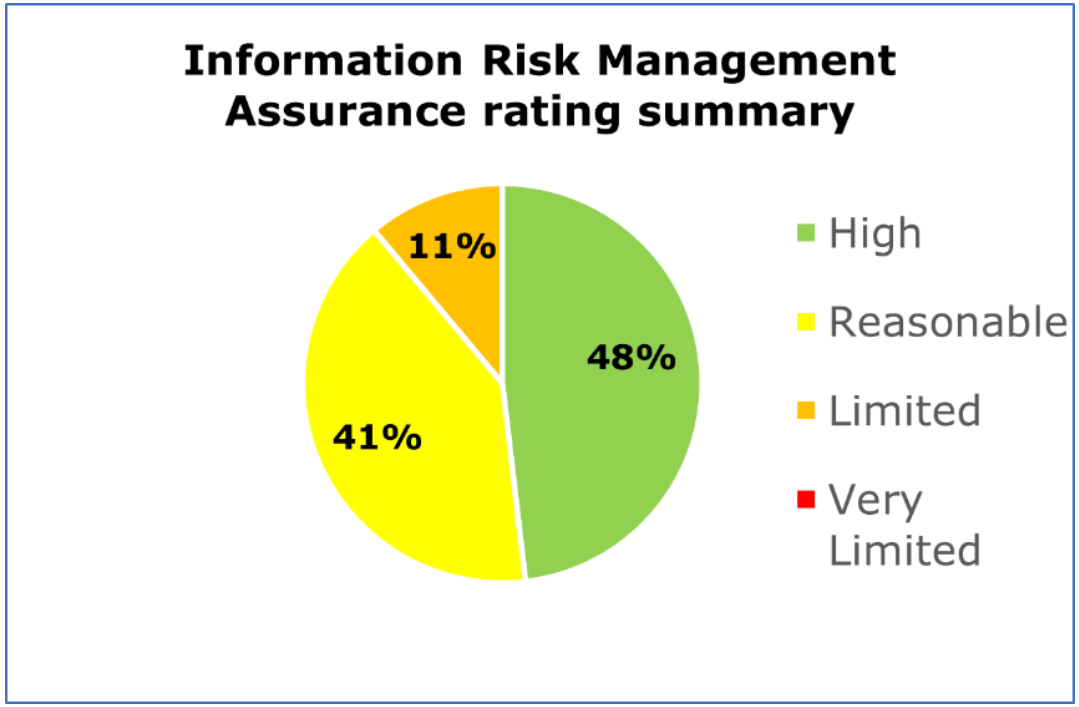
- Records Management has 3 urgent, 18 high and 10 medium priority recommendations.
- Information Risk Management has 11 high and 3 medium priority recommendations.
- Personal Data Breach Management and Reporting has 1 urgent, 7 high, 3 medium and 1 low priority recommendations.

Graphs and Charts



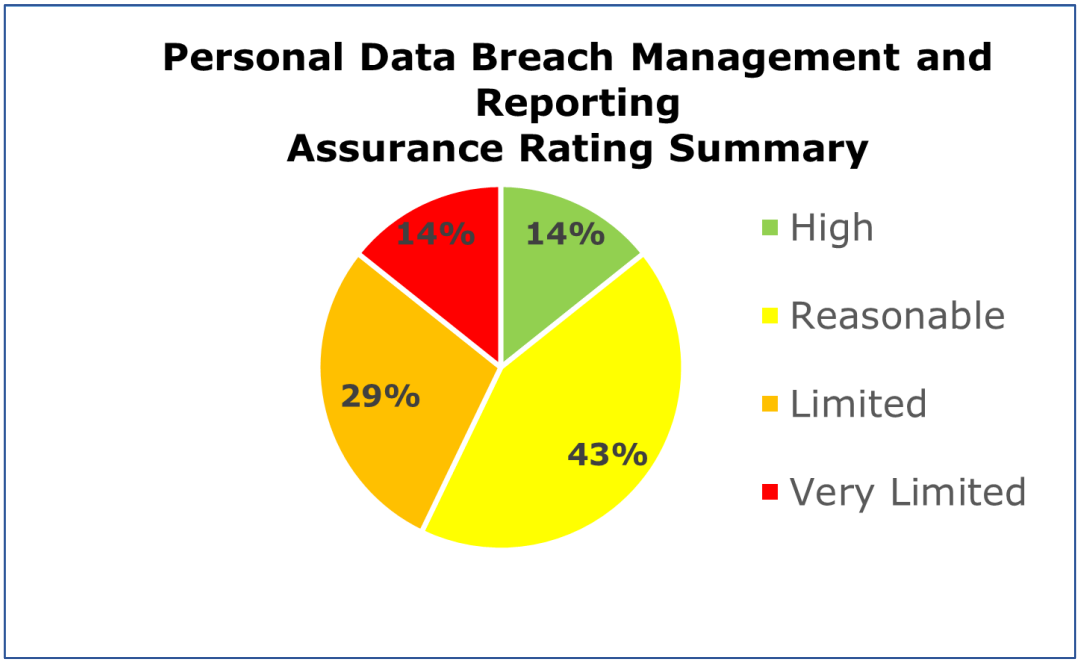
The pie chart shows the percentage breakdown of the assurance ratings given for the Records Management scope:

- 26% high assurance
- 12% reasonable assurance
- 33% limited assurance
- 29% very limited assurance



The pie chart shows the percentage breakdown of the assurance ratings given for the Information Risk Management scope:

- 48% high assurance
- 41% reasonable assurance
- 11% limited assurance



The pie chart shows the percentage breakdown of the assurance ratings given for the Personal Data Breach Management and Reporting scope:

- 14% high assurance
- 43% reasonable assurance
- 29% limited assurance
- 14% very limited assurance

Areas for Improvement

Roll out the Records Management (RM) training to all staff across the IOPC. Ensure job roles with additional requirements such as the retention and disposal of records receive specialist training in this area. Expand the Training Needs Analysis (TNA) to encompass all job roles with additional requirements, including information risk management. The content of the training should link into existing information risk/RM policies and procedures to strengthen compliance in these areas.

The Information Asset Register (IAR) and Record of Processing Activities (ROPA) should be routinely audited to ensure all the required fields are populated, and the relevant requirements are included as listed within Article 30 UK GDPR and s.42(4), 61 DPA18. The ROPA should also indicate whether personal data is being retained or erased in line with the IOPC's appropriate policy document (APD).

Initiate a programme of internal audits to ensure compliance with UK GDPR and DPA18. Audits should include an assessment of the measures in place to detect personal data breaches, data quality reviews and the security controls of areas which store in-house physical records.

Ensure the new InfoSec policy is ratified and approved by the Information Assurance Board (IAB) and subject to regular review. Produce a formal Access Control policy which details how access to information systems is granted across the IOPC.

Review electronic records within shared drives which contain personal data to ensure they are being stored within the appropriate repository. Ensure guidance for the storage of all documents across the IOPC is ratified and approved.

Review all legacy files to determine whether these should be marked for permanent preservation or disposed of in accordance with the Retention and Disposal schedule. Begin to review active and archived records held both physically and electronically to ensure compliance with the storage limitation principle.

Conduct audits and inspections at Iron Mountain to ensure the security of records held at this facility is maintained, and that records which are disposed of off-site are done so securely. This will enhance compliance of Article 5(1)(f), 28 UK GDPR and s.40, 66 DPA18. Review the sharing of personal information with third party organisations to determine the data processing relationship and ensure that the appropriate contracts or agreements are in place. These agreements should include each parties responsibility for the management and reporting of personal data breaches.

Develop guidance for staff with responsibility for personal data breach management to follow in the event of a security incident. This guidance should include the management and recording of near-miss incidents, determining whether a personal data breach has occurred, notifying affected parts of the organisation, reporting the breach to the ICO, notifying affected individuals, identifying root causes and the procedure for the management of 'out of hours' breaches.

Develop a Data Protection Impact Assessment (DPIA) policy to ensure the process for conducting DPIA's is consistent across the IOPC and sufficient to meet the requirements of UK GDPR and the DPA18. Ensure the policy includes information on assigning DPIA's formal review dates so new risks which may emerge are identified and controlled at the earliest opportunity.

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 IOPC.

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