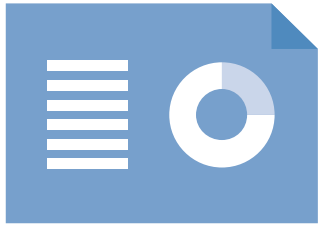
# Legal Ombudsman

## Data protection audit report

June 2019

ico.
Information Commissioner's Office

# Executive summary



## Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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 Legal Ombudsman (LO) agreed to a consensual audit by the ICO of its processing of personal data. The on-site audit was undertaken at LO premises: Edward House, Quay Place, Birmingham, B1 2RA and included a visit to the off-site archive storage facility provided by Boxit.

The purpose of the audit is to provide the Information Commissioner and the LO with an independent assurance of the extent to which the LO within the scope of this agreed audit, is complying with data protection legislation.

It was agreed that the audit would focus on the following area(s):

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

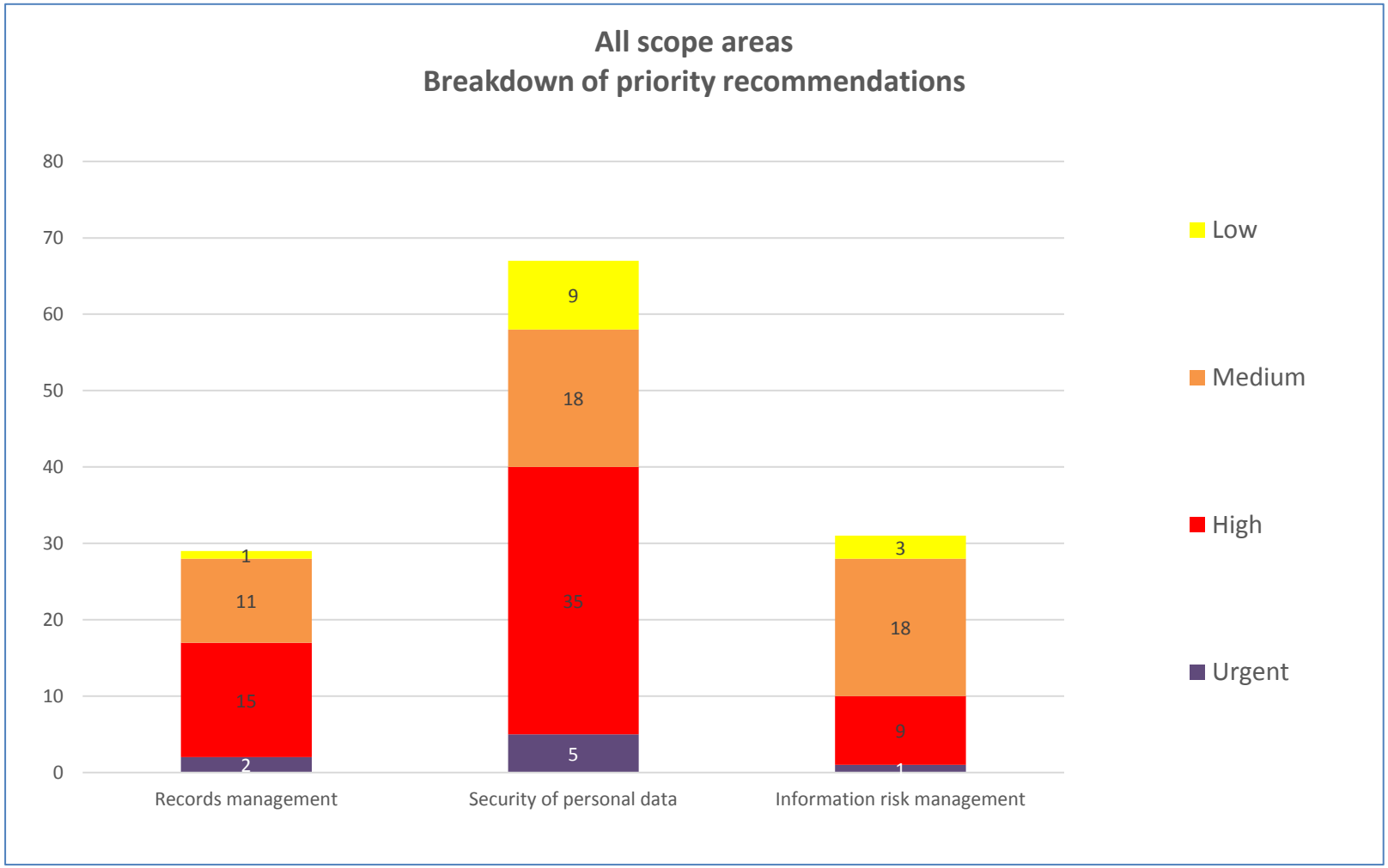
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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 LO 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 LO priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

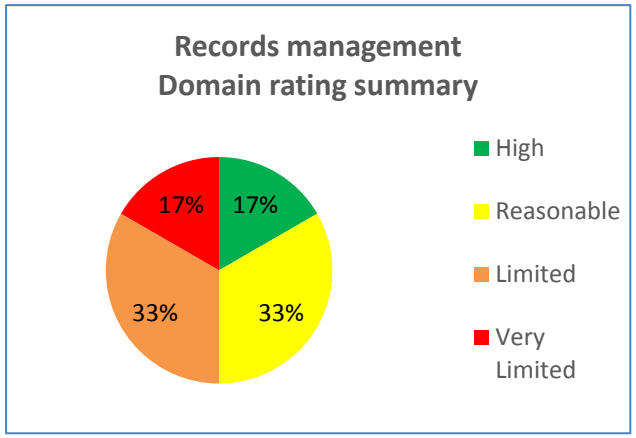
## Audit Summary

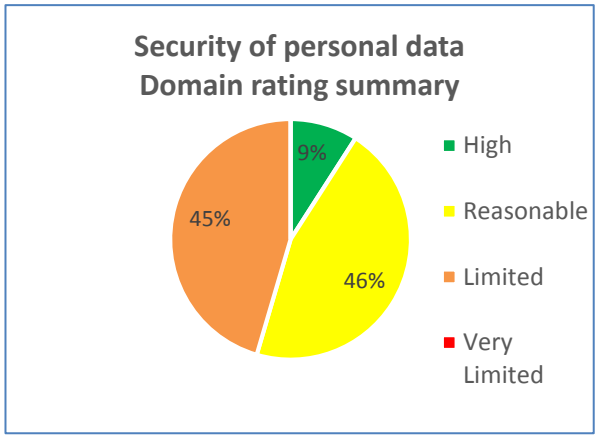
| Audit Scope Area | Assurance Rating | Overall conclusion |
|---|---|---|
| Records Management | LIMITED | There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation. |
| Security of personal data | 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. |
| Information Risk 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. |

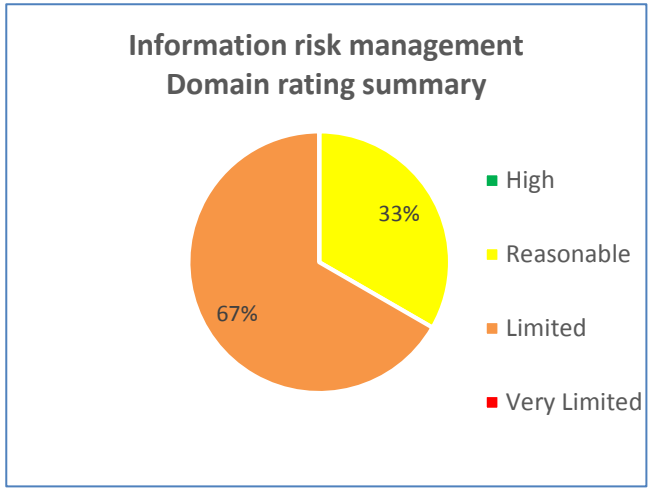
# Priority Recommendations



# Graphs and Charts



## Areas for Improvement

A number of issues were identified regarding the physical security of both LOs main office and their third party document storage. To remedy these issues the LO should carry out a review of ways it can prevent unauthorised access to its premises. The LO should also work with their third party document storage to improve the physical security of their paper records.

Not all LO records are currently disposed of in line with the Retention Schedule, as a number of staff expressed lack of familiarity or a belief it was needlessly complex. This has resulted in the LO continuing to process substantial amounts of personal data which may no longer be required.

The LO has not carried out a data flow mapping exercise or information asset audit, and the Information Asset Risk Registers which are used do not provide either sufficient detail or governance oversight. Without having a data flow map which documents records of all processing activities in place, the LO lacks the documentation necessary to comply with Article 30 of the GDPR and should take immediate steps to resolve this.

There is a lack of oversight of the services provided to the LO by their third party IT provider. The LO cannot show that they have assurance from the IT provider that they are adequately carrying out their network management responsibilities, for example in providing effective anti-virus and anti-malware protection.

Information Asset Owners (IAOs) were found to require refresher training on how to assess risk and complete risk registers. Some IAOs were also unaware of their responsibilities in managing document retention. Moreover, the overall effectiveness of the general training programme was questioned during the audit. The LO should take steps to ensure that their training regime leaves their staff prepared to carry out all relevant duties.

## Good Practice

The LOs Data Quality team use extensive and granular exception reporting to carry out highly accurate quality reviews of information held on the Case Management System (CMS). Carrying out these reviews assists the LO in meeting their obligations under Article 5 of the GDPR to ensure the accuracy of the information they process.

## 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 Legal Ombudsman.

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