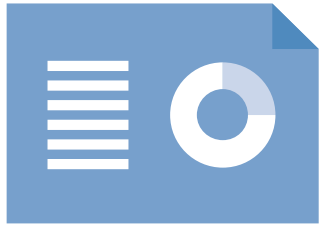
The Crown Prosecution Service

Data protection audit report

December 2019

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.

An assessment notice dated 9/8/19 was issued to the Crown Prosecution Service (CPS) in order for a compulsory audit to take place. The on-site audit was undertaken at the CPS Headquarters in Petty France London and local area and divisional offices in the East Midlands, North East and York.

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

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

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
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 Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Training & Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.

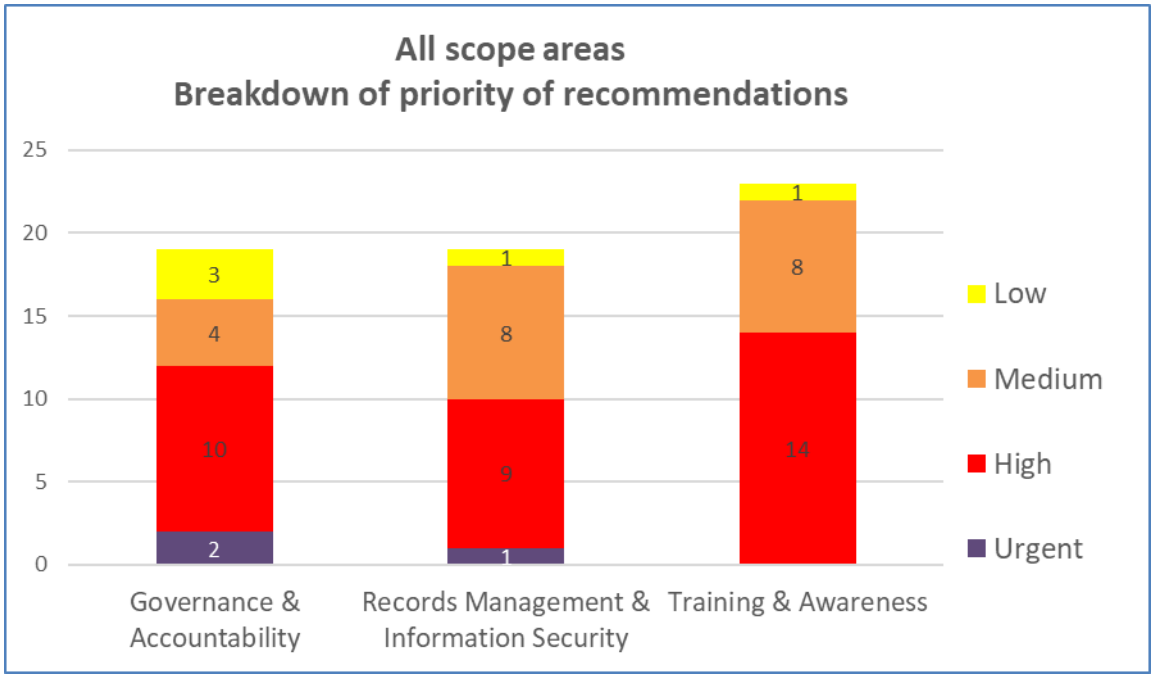
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

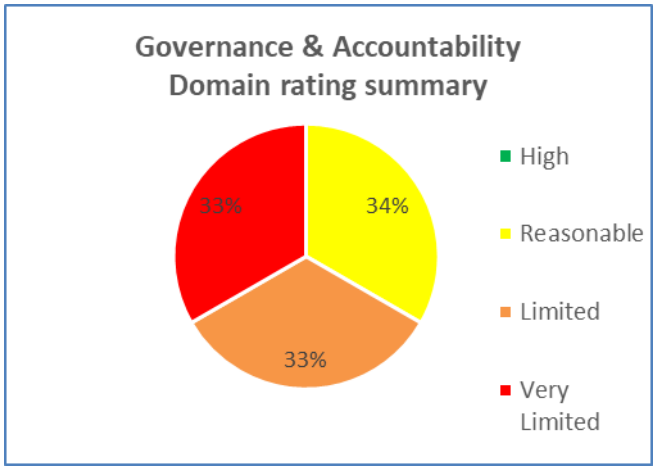
Audit Summary

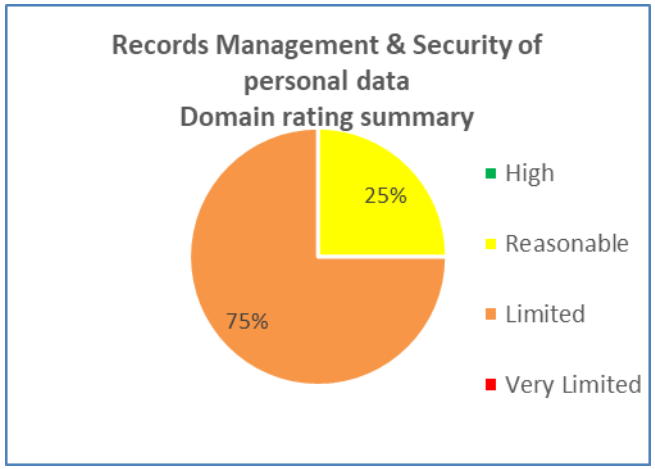
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management & 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.
Training & Awareness	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.

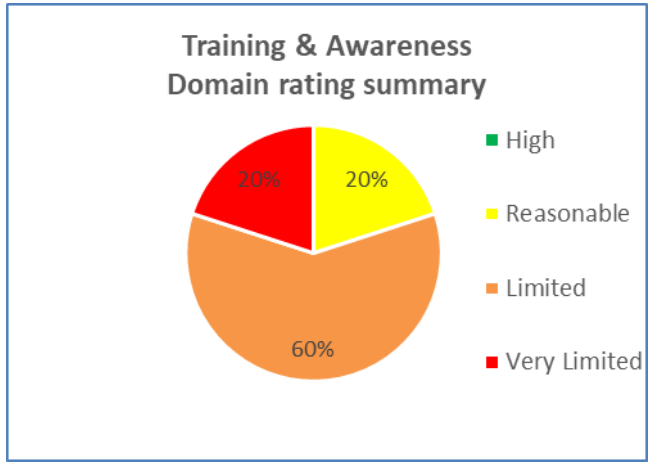
Priority Recommendations



Graphs and Charts







Areas for Improvement

The CPS does not have a formal steering group that has oversight of all information governance (IG) performance and activities across the whole organisation. Reporting mechanisms to the Data Protection Officer (DPO) and Senior Information Risk Owners (SIROs) need to be reviewed. Information risk processes and responsibilities are not specified in policies. Risks involving CPS data processing activities are not being adequately assessed, recorded and managed.

The CPS do not have an appropriate policy in respect to its sensitive/special category data processing as required by the DPA 18 and there is no policy to cover data sharing activities. Work is underway to review and update existing IG policies, but this is still in its infancy.

The procedures for granting, monitoring and restricting access to removable media are not currently formally documented. There is insufficient oversight of staff's use of removable media and their ability to download personal data.

The Incident Management and Reporting Policy requires updating to ensure that it is up to date and fit for purpose. Processes and responsibilities for responding to incidents and managing them should be documented including internal escalation and reporting to the ICO and data subjects where appropriate.

There is no overall, sector specific, IG training programme covering data protection, GDPR, records management or data sharing; this means that the CPS have limited assurance that staff are suitably trained to carry out their roles effectively. There are limited resources available to deliver IG training resulting in a lack of a clear strategy to meet training needs and inconsistencies in training levels across the organisation.

Induction training is insufficient to meet the needs of staff and there is a lack of role-specific training for staff in specialist roles. In addition, responsibility for following up on non-completion of training is not clearly defined and no action is taken to ensure completion; as a result, refresher training completion rates consistently fall short of targets.

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