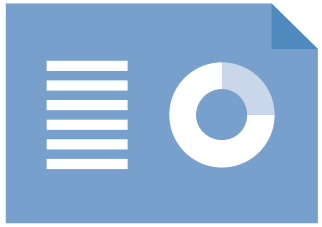
Essex Police

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.

Essex Police (EP) agreed to a consensual audit by the ICO of its processing of personal data. The on-site audit was undertaken at EP Headquarters, Sandford Road, Chelmsford CM2 6DN and at their in-house records document storage facility.

The purpose of the audit is to provide the Information Commissioner and EP with an independent assurance of the extent to which EP, 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
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.
Requests for Personal Data	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

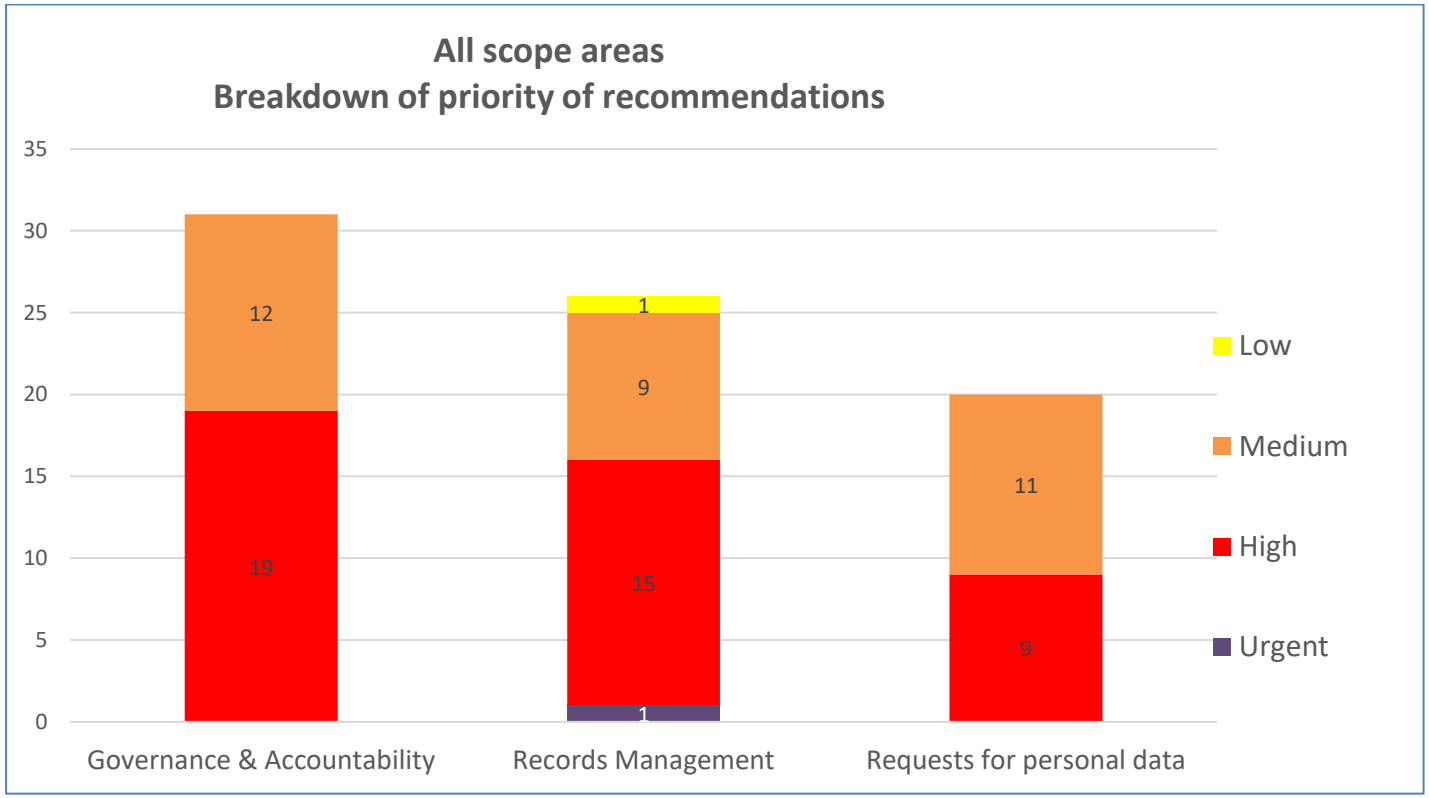
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist EP 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. EP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

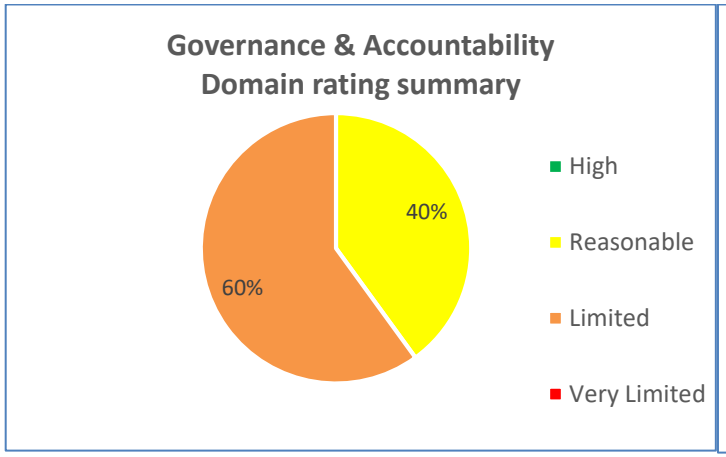
Audit Summary

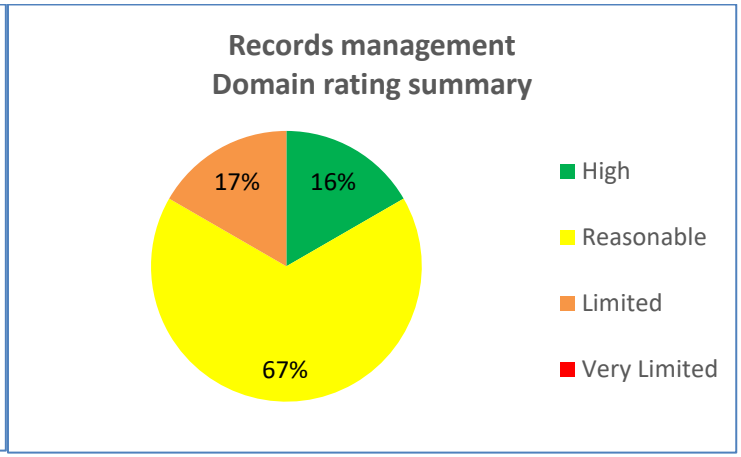
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to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

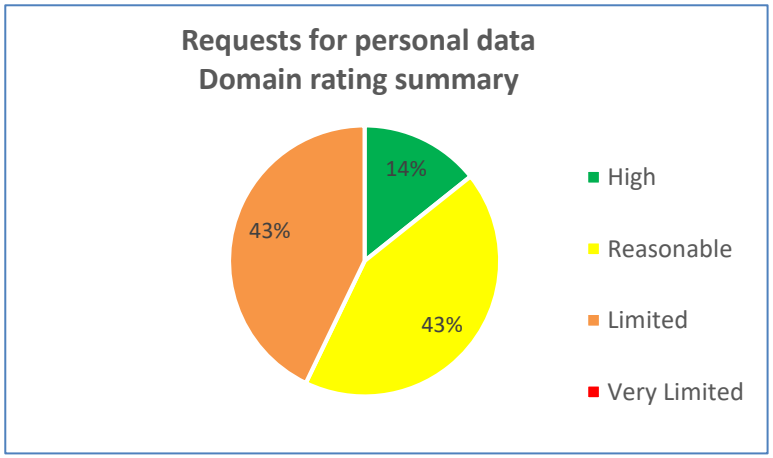
Priority Recommendations



Graphs and Charts







Areas for Improvement

Produce comprehensive and clear privacy notices so that individuals are aware why their data is being processed, under what lawful basis and what rights they have in relation to that processing, including the right to withdraw consent at any time. The privacy information should be available in other languages and formats to meet the needs of all sections of society.

A comprehensive Record of Processing Activities/Information Asset Register covering the whole organisation will enable strategic oversight of information risks and a quality assurance check will be required to ensure consistency. This is required to be compliant with Article 30 GDPR and Section 61 DPA18 legislation. Information Asset Owners and Assistants should have their records management responsibilities formally documented in the job description to reflect the importance of the role.

The current Information Governance training programme for all staff needs to be upgraded to cover key data protection areas. Training programmes are required for specialised roles, including records management and handling requests for personal data. This would equip key staff with the detailed knowledge they need to fulfil their data protection responsibilities. Regular refresher training should also be scheduled and implemented.

Written contracts and agreements are yet to be identified and put in place with all data processors, along with the compulsory details and terms and conditions as outlined in the GDPR, including information security requirements, rights of the individual and compliance checks/audits. In addition, to identify and manage information risks, a programme of risk based information governance audits should be included in the internal audit plan.

Periodic audits of the in-house records storage and third-party records disposal facilities should be scheduled on a regular basis to assure Essex Police that agreed standards are being met. Before records are disposed of there should be a documented record of management approval.

Physical records are not adequately tracked. Without robust tracking procedures in place the risk that the documents could be unlawfully accessed, compromised or lost is greatly increased. Also, should there be a breach of special category data the harm to the data subjects is substantially higher.

Documented procedures to allow rights of individuals to request deletion or erasure of their information should be updated to be compliant with Article 17 GDPR and Section 47 of DPA18.

To facilitate requests for personal data, the external website should reflect that requests for personal data can be made verbally. Information should undergo a review by a peer or senior member of the team prior to issue, covering letters should detail any searches conducted and letters of refusal should advise them of their right to appeal/complain to the ICO. Reviews/dip sampling of completed requests should take place to ensure that procedures have been followed correctly and to identify any areas for improvement.

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