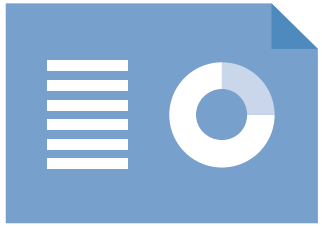
Scottish Police Authority

Data protection audit report

December 2018

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.

This audit was conducted as part of the audit follow up procedure following the previous audit which took place in August 2017. The purpose of the audit is to provide the Information Commissioner and the Scottish Police Authority (SPA) with an independent assurance of the extent to which SPA, 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**
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.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
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.

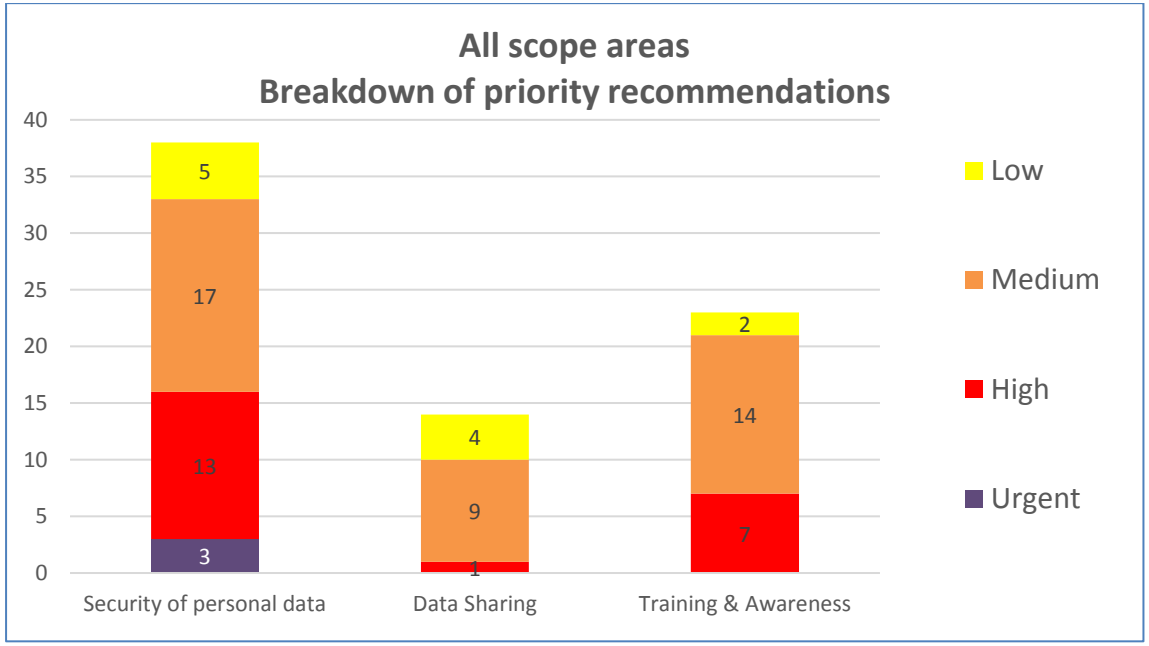
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

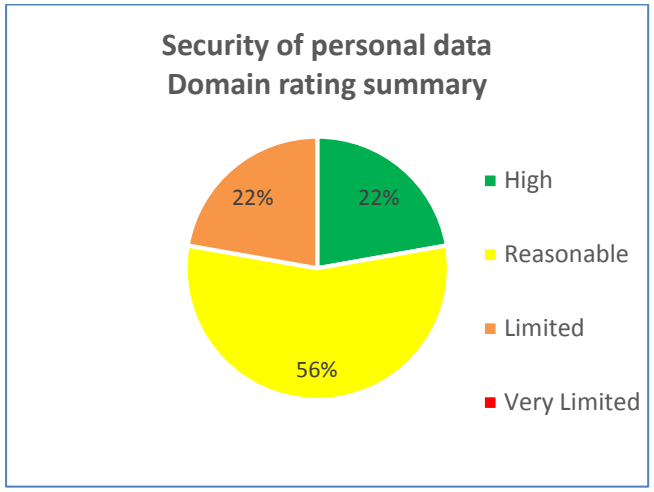
Audit Summary

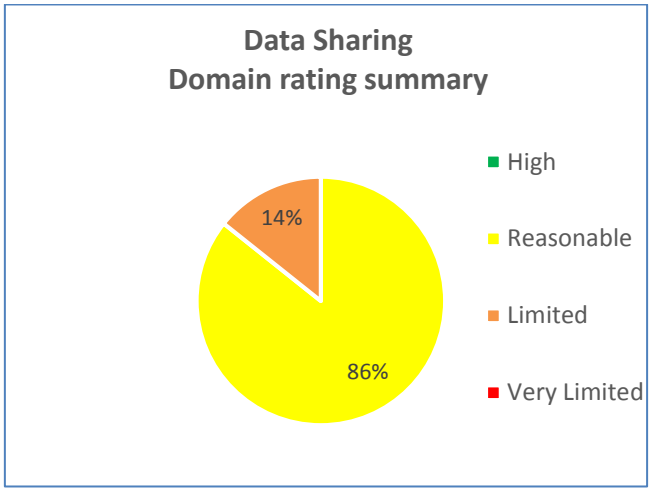
Audit Scope Area	Assurance Rating	Overall Opinion
Security of personal data	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	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.
Training & Awareness	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.

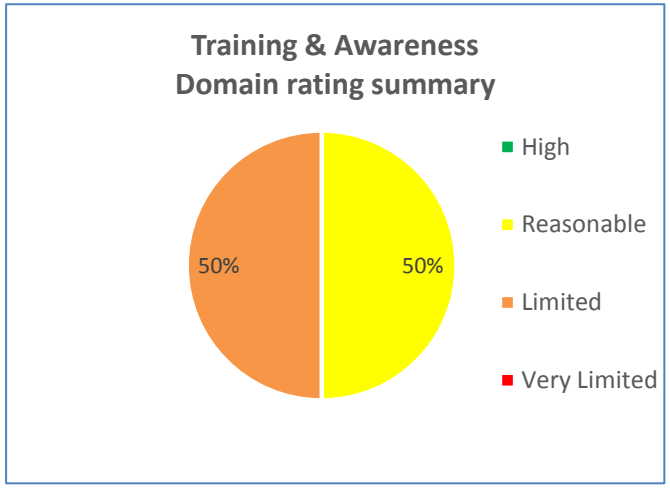
Priority Recommendations



Graphs and Charts







Areas for Improvement

- SPA should seek to urgently put in place a contract with Police Services of Scotland (PSoS) for the provision of IT services, including Service Level Agreements and Quality Standards in order to provide assurances that those services will continue to be delivered at an acceptable standard.

- SPA should take steps to ensure that all incidents and breaches across the organisation are dealt with using SPA procedures, including those breaches and incidents which take place within the Forensic Services Department.

- SPA should take immediate action to ensure that all systems and hardware are running up to date antivirus software.

- SPA should ensure that all staff who have the option to work remotely have read and understood the Remote Working Policy, and that their acceptance of the policy is recorded.

- SPA should ensure that data sharing agreements (DSAs) are reviewed on a regular basis to provide assurance that they are operating effectively and that all parties are complying with their obligations.

- SPA should ensure that regular data quality checks are carried out in relation to shared data to ensure that inaccurate data is being identified and updated or amended as necessary and that sharing partners are kept informed.

- The information security e-learning module completed by staff in Forensics has not been updated to reflect current data protection legislative requirements.

- SPA do not have a documented training strategy or plan in place at present.

- SPA should ensure that specialist training is provided to their Information Asset Owners.

- Although not within the scope of this audit, it was brought to the attention of ICO auditors that contracts with third parties are procured by PSoS in SPA's name. SPA should ensure that they have sufficient oversight of these contracts to gain assurance that they contain the necessary clauses and provisions in order for them to be compliant with data protection legislation. This includes ensuring staff employed by third party contractors have received data protection

training appropriate to their roles.

Good Practice

- The appointment of Clear Desk Champions by Forensic Services has ensured that areas which are not regularly visited by IM staff continue to engage fully with the Clear Desk Policy. This has also helped to raise staff awareness of information security procedures.

- The comprehensive nature of the IT Threat Monitoring is particularly good practice. By taking information from such a varied selection of media and sources, SPA have assurance that any upcoming vulnerability will be spotted by the IT team.

- SPA have developed comprehensive Standard Operating Procedures for data sharing and work is underway to ensure that they are put into practice.

- SPA have developed a Data Sharing Agreement Register which records key details about each agreement, including the organisations involved, the data that is shared, and the legal basis for sharing.

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 SPA.

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