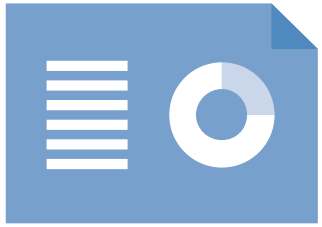
Wiltshire Police

Data protection audit report

February 2020

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.

Wiltshire Police (WP) agreed to a consensual audit by the ICO of its processing of personal data. The on-site audit was undertaken at WP Headquarters, London Road, Devizes SN10 2DN and at Swindon Police Station Gablecross, Shrivenham Road, Swindon SN3 4RB.

The purpose of the audit is to provide the Information Commissioner and WP with an independent assurance of the extent to which WP, 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.
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.
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.

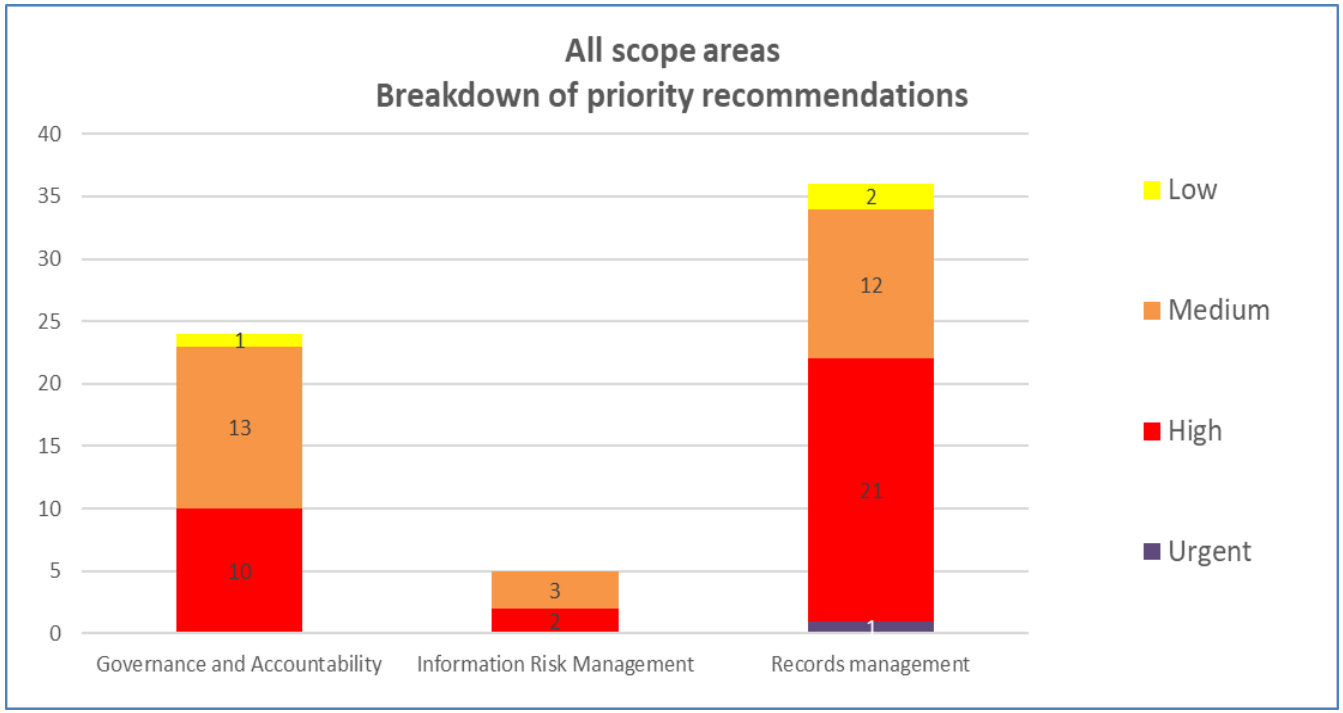
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

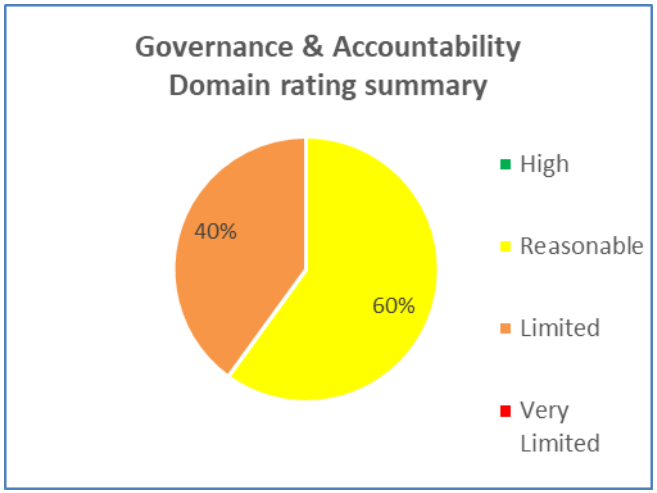
Audit Summary

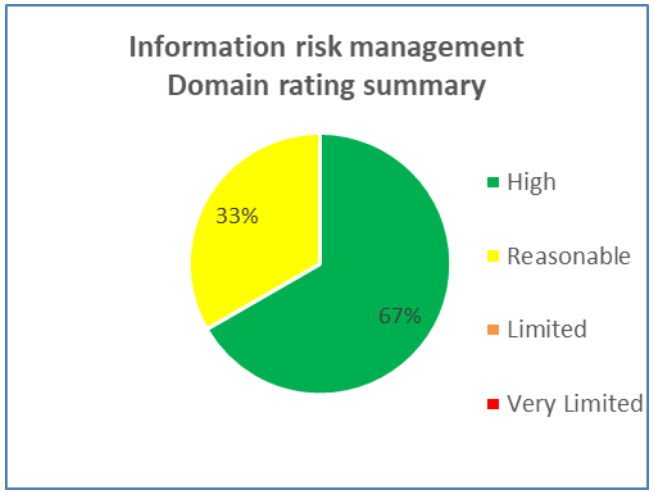
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Risk Management	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
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.

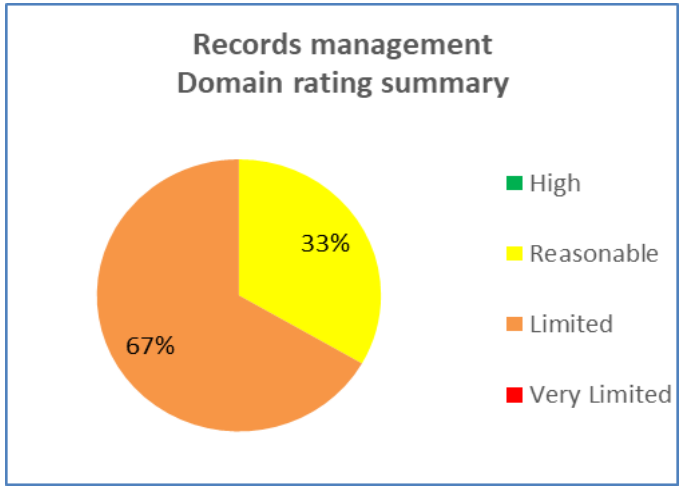
Priority Recommendations



Graphs and Charts







Areas for Improvement

- Develop and implement a formal sign off process to gain assurance that staff have read new and amended data protection (DP) policies and understood current Information Governance (IG) related guidance and procedures.

- Develop an overall information management training policy which tailors training to individual job role requirements, and provide specialist training to staff responsible for records management (RM), information security (IS), data protection (DP), disclosures, data sharing and data protection impact assessments (DPIAs). This would equip key staff with the detailed knowledge they need to fulfil their data protection responsibilities.

- Routinely monitor the compliance with Information Governance (IG) policies of any processor acting on behalf of WP. This should cover the processor's procedures, DP training and data security arrangements to ensure they are effective and comply with contractual agreements. In addition, to identify and manage information risks, a programme of risk based IG audits should be initiated as part of an internal audit plan.

- The Record of Processing Activities/Information Asset Register covering the whole organisation needs to be completed. This will provide a strategic oversight of information asset risks and enable compliance with Article 30 GDPR and Section 61 DPA18 legislation.

- Review all consent mechanisms to ensure they meet GDPR requirements. There should be clear, publicised information on how individuals can withdraw their consent and when such requests are received they are acted upon promptly.

- Document procedures for records management for all areas of the organisation. There is a risk that records are not appropriately classified, stored and disposed of.

- A contract should be put in place for the IT services provided by a third party. The contract should cover all aspects of processing carried out and be compliant with Article 28 of the GDPR.

- Periodic audits of the in-house records storage and third-party records disposal facilities should be scheduled on a regular basis to assure WP 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.

Best Practice

Information risks are held within one database which provides access to both the local risk register owned by each Information Asset Owner (IAO) and the Force risk register. Risks are assessed locally using a risk matrix and those risks scoring higher than 30 appear on the Force risk register. The risk register is monitored by a continuous improvement leader who sends monthly reminders to review their information asset risks.

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