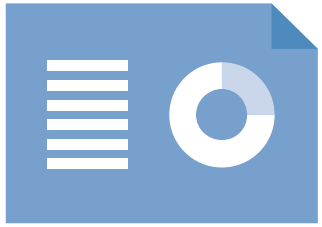
West Midlands Police Birmingham

Data protection audit report

July 2018

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the General Data Protection Regulations (GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision 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 purpose of the audit is to provide the Information Commissioner and West Midlands Police (WMP) with an independent assurance of the extent to which WMP, 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 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 and 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.

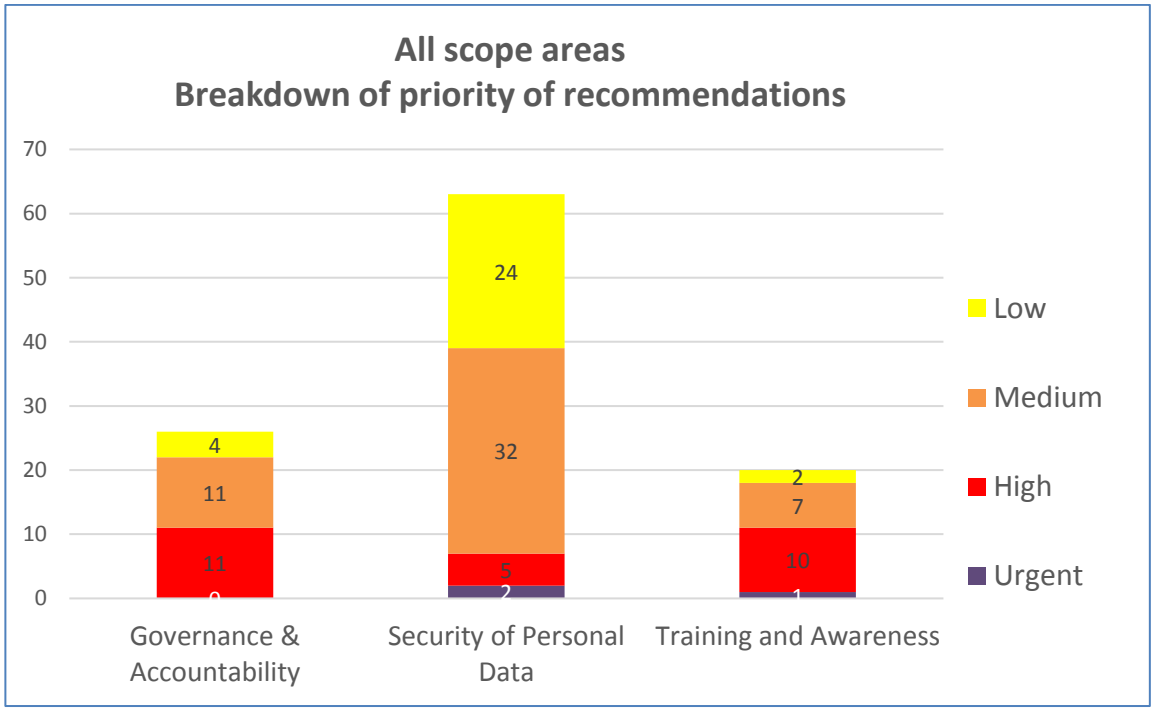
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

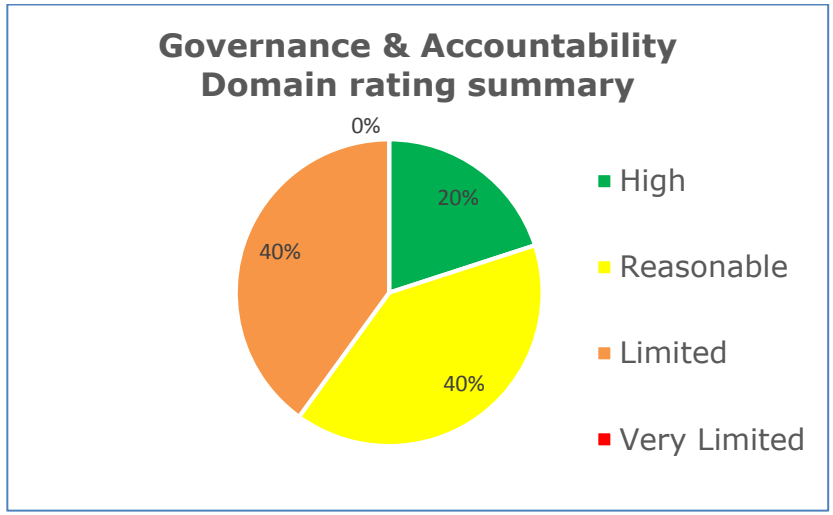
Audit Summary

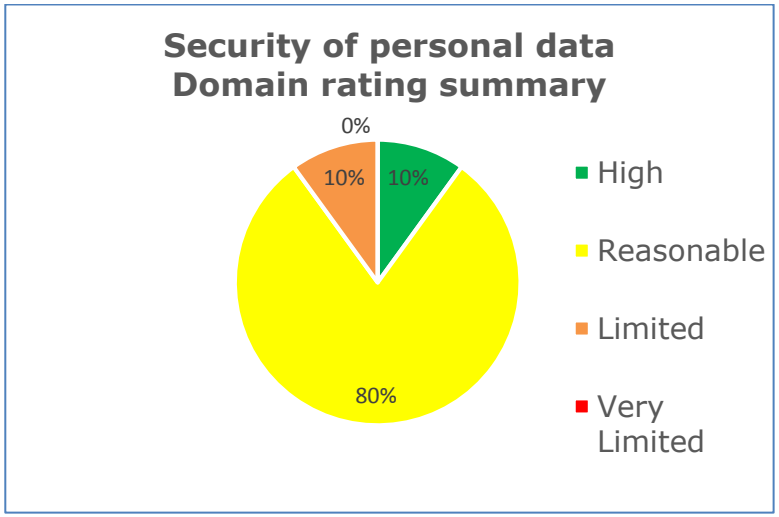
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce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

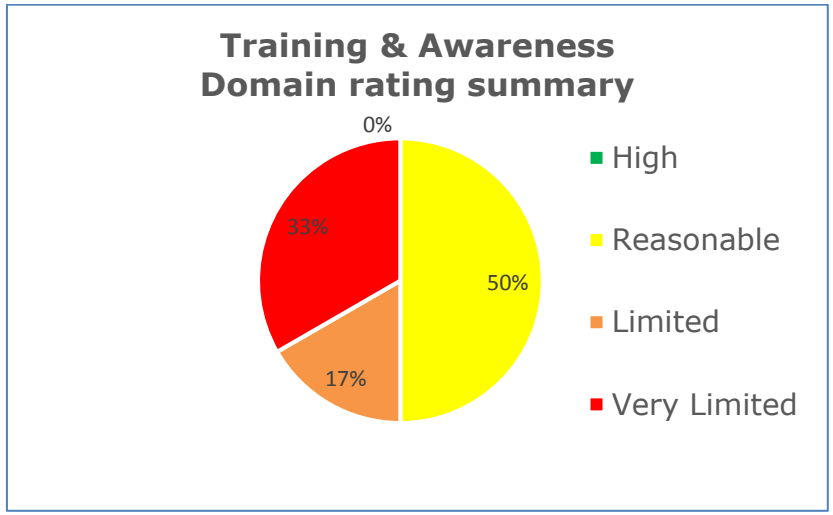
Priority Recommendations



Graphs and Charts







Areas for Improvement

- Although WMP have a defined process implemented for reviewing, ratifying and approving policies in place, it is not effective. WMP should ensure that all of their existing policies are reviewed, ratified and approved periodically and kept up-to-date, so that any risks can be reviewed and policies adapted in line with new legislation.
- Staff can log on to the network using with both their smartcard and PIN and their username and password. It is possible for a user to be logged in on 2 different desktops at the same time using the different methods.
- There is a lack of documented operating procedures detailing information security (IS) practices throughout the Force. These procedures should be regularly reviewed.
- The incident management procedure is currently in draft form. It is unclear how staff are aware of the need to report IS incidents that do not involve IT equipment.
- WMP should provide all staff who have access to locations where sensitive material may be encountered, with information governance training. This would give WMP an assurance that all staff are aware of the sensitivity of work undertaken and all their responsibility to WMP and the legislation.
- WMP have no Training Needs Analysis (TNA) available for staff and officers outside of national TNA for police officers. WMP should undertake a TNA to find and plug any gaps in knowledge for their staff, in particular reference to those who access personal data or have specific data handling and security management responsibilities. A TNA would then enable them to plan ahead for additional training needs and budgetary costs.
- WMP should create an assessment with an appropriate pass rate that all staff should complete on the completion of their NCALT training. This would give WMP an assurance that they have understood the training and their responsibilities under the legislation and that the training is effective.
- WMP should ensure that sufficient resources are available in the relevant department to produce KPIs so that training completion can be monitored.

Good Practice

- The process in the Occupational Health Team of explaining consent and allowing an individual to withdraw at any stage of the process is extremely well thought out and clear.
- All policies contain a statement reminding readers that printed versions should not be relied on and that most up to date versions can be found on the intranet.
- WMP have recently decided to insist that body worn cameras used by Police Officers are encrypted following a risk assessment. It was reported that they are the only Police Force to insist on this requirement.
- WMP have three easily identifiable types of ID cards, black for WMP staff, yellow for contractors which includes Police Officers from other forces and red for visitors. This alerts staff, including security personnel and helps to ensure that only appropriate access is granted.
- The use of an automated system to dynamically review the allocation of access rights every 15 minutes means that changes to and removals of those rights can be implemented promptly and efficiently. This will provide assurance against unauthorised access to personal data.
- The GDPR project team produced Information Asset Owner (IAO) training and identified IAO needs and concerns through a questionnaire and then IAO handbook. The handbook identifies and highlights issues across a wide range of directorates and departments. IAOs interviewed as part of the audit have really appreciated the help and ongoing training.

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