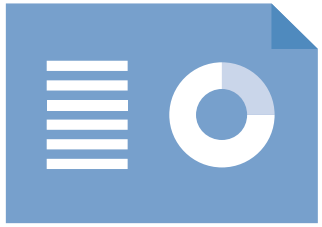
West Mercia Police

Data protection audit report

December 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.

West Mercia Police (WMP) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 4 August 2020 with representatives of WMP to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and West Mercia 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 and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance with Part 3 of the DPA 2018 are in place and in operation throughout the organisation.
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their 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.

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

However, due to the outbreak of Covid-19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, WMP agreed to continue with the audit on a remote basis. A desk-based review of selected policies and procedures and remote telephone interviews were conducted from 26 October to 12 November 2020. The ICO would like to thank WMP for its flexibility and commitment to the audit during difficult and challenging circumstances.

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

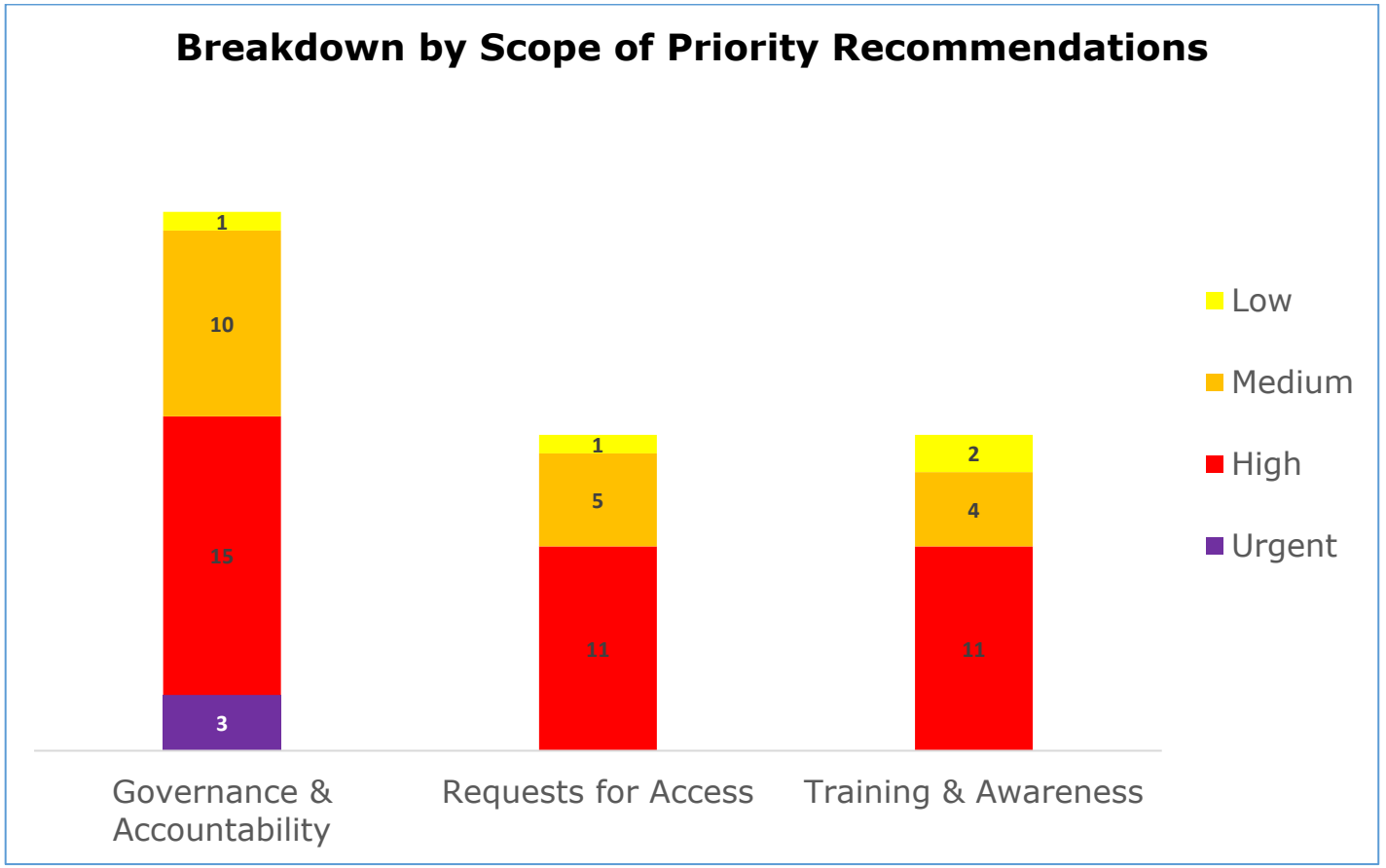
been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. WMP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary*

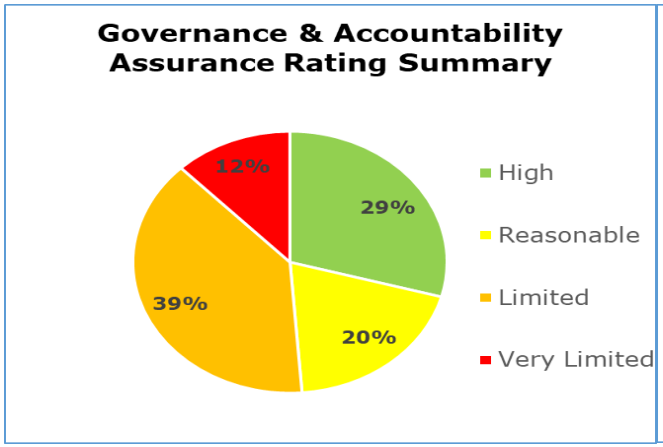
Audit Scope Area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to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

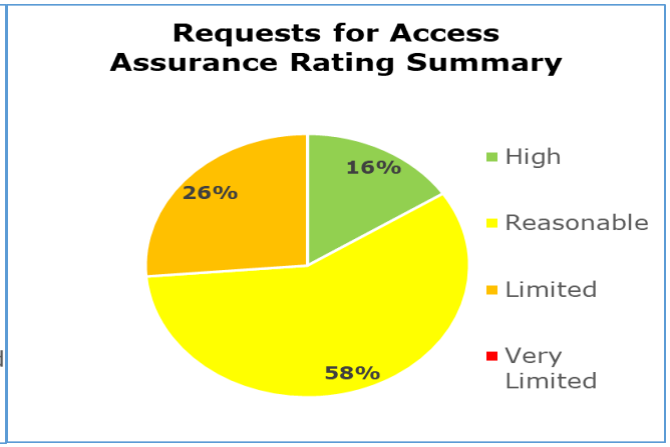
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

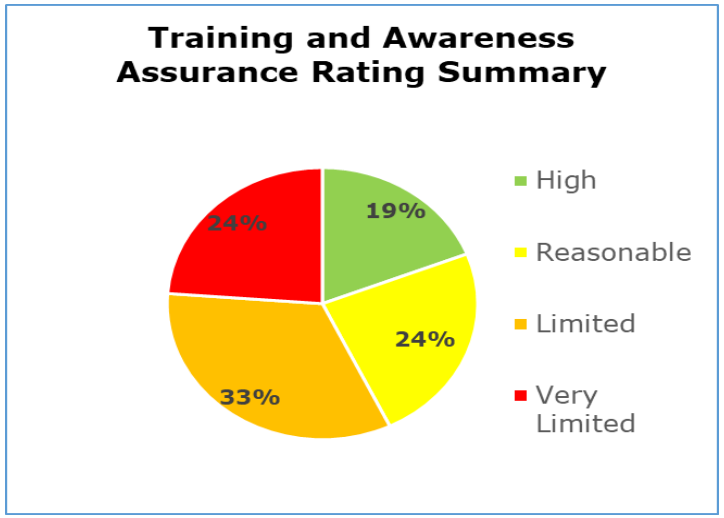
Priority Recommendations



Graphs and Charts







Areas for Improvement

Logging of automated processing systems (any IT database) needs to be completed for all WMP systems to meet section 62 of the DPA 2018 requirements. The effectiveness of any processors logging systems should also be routinely checked.

A programme of risk-based information governance (IG) audits should be initiated as part of an internal audit plan. Risk identification and management can be augmented by a regular programme of independent external audits.

All law enforcement data processing arrangements should be supported by up to date written contracts, regularly reviewed, that comply with the requirements of the DPA 2018.

Complete a data mapping exercise for all information assets and processing activities, to create an overarching record of processing activities (ROPA). The exercise is key to comply with section 61 of the DPA18 legislation and establishing the lawful basis for processing personal data and sensitive processing.

Data protection policies and procedures require reviewing on completion of the ROPA to ensure that sufficient guidance is available to inform staff of their responsibilities in relation to data minimisation**,** including any review of information asset registers and retention schedules. This should include the retention period for emails.

Establish a process to gain assurance that WMP staff have read and understood relevant data protection policies and procedures, combined with regular monitoring of staff compliance with the procedures.

Data protection impact assessments (DPIAs) should be completed before any high risk processing of personal data takes place. All DPIAs should be assigned a formal review date or an early review instigated when a substantial change to the nature, scope, context, or purposes of the process occurs.

Develop a needs based training programme which identifies and addresses the training requirements of all staff, volunteers and contractors, in relation to IG compliance. The DPO should have oversight of the force IG training to ensure sufficient and appropriate content.

Ensure that IG refresher training is completed by all staff, volunteers and contractors regularly, in line with College of Policing Authorised Professional Practice, ensuring that key performance indicators (KPIs) are updated accordingly.

Request for access procedures should be improved to detail how WMP staff should handle requests for access to personal information and to ensure they reflect both general processing under the GDPR and Part 3 law enforcement processing of the DPA18.

The disclosure information provided to data subjects should explain the searches WMP have undertaken and an overview of what information has been provided as a result of those searches.

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 WMP.

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