Avon and Somerset Police

Data protection audit report

June 2024

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Avon and Somerset Police (A&S) agreed to a consensual audit of its data protection practices

The purpose of the audit is to provide the Information Commissioner and A&S with an independent assurance of the extent to which A&S within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of A&S's processing of personal data. The scope may take into account any data protection issues or risks which are specific to A&S identified from ICO intelligence or A&S's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of A&S the nature and extent of A&S's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to A&S.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate

Audits are 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, remote interviews with selected staff, and a virtual review of evidential documentation.

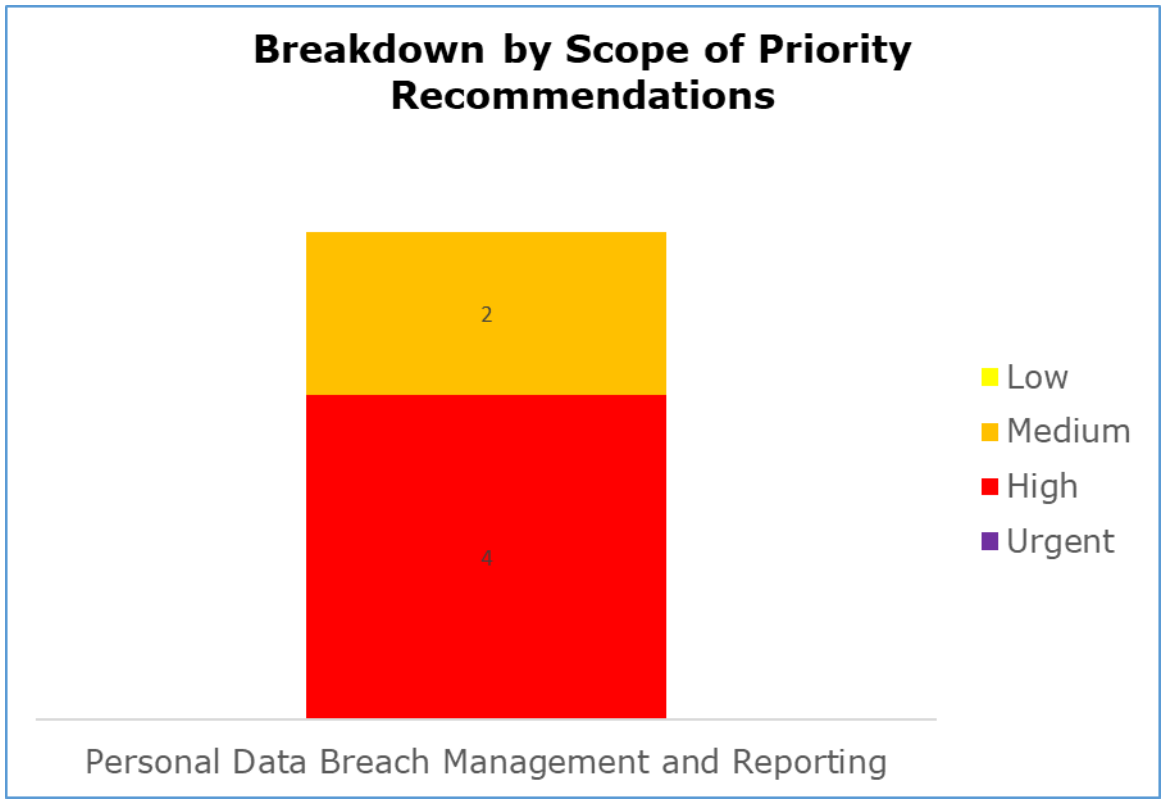
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist A&S in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. A&S'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
Personal Data Breach Management and Reporting	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.

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

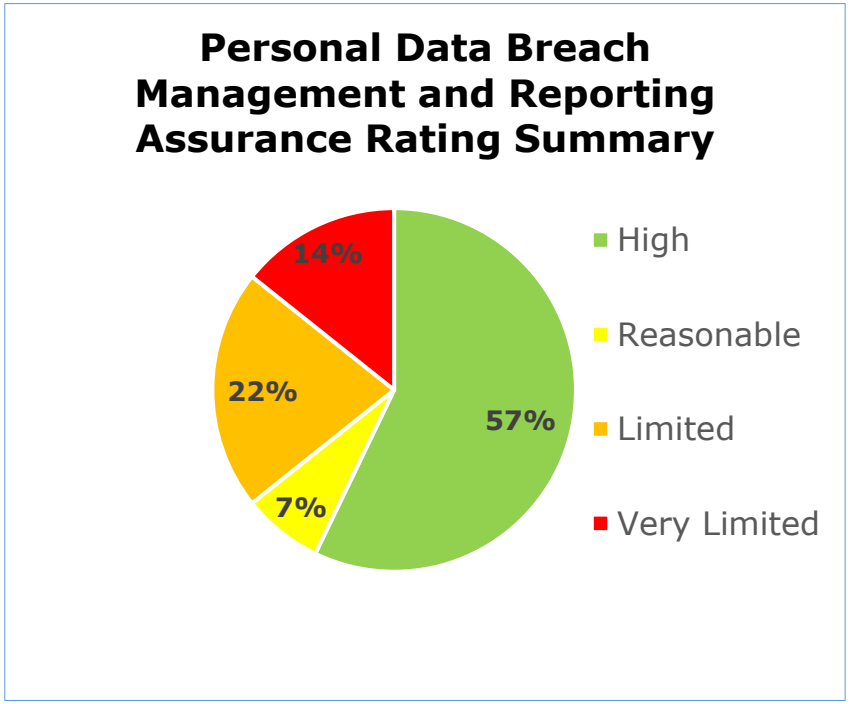
Priority Recommendations



The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Four high and two medium priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management and Reporting scope. 57% high assurance, 7% reasonable assurance, 22% limited assurance, 14% very limited assurance.

Areas for Improvement

- Complete a training needs analysis for all staff that may be involved in making decisions about security incidents and personal data breaches. Ensure that the required training identified is completed and refreshed at an appropriate frequency.
- Review the data breach logs regularly to ensure there is a defined retention period that is being adhered to and data minimisation techniques are being applied correctly.
- Ensure any collective learnings identified from data breaches are shared across the whole organisation.

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