Police Service of Scotland

Data protection audit report

September 2023

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 (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 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.

Police Service of Scotland (PSoS) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 21 March 2023 with representatives of PSoS to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and PSoS with an independent assurance of the extent to which PSoS, 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 PSoS's processing of personal data. The scope may take into account any data protection issues or risks which are specific to PSoS, identified from ICO intelligence or PSoS's own concerns, and/or any data protection issues or risks which affect their 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 PSoS, the nature and extent of PSoS's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to PSoS. It was agreed that the audit would focus on the following areas:

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 with Part 3 of the DPA18 and other national data protection legislation are in place and in operation throughout the organisation.
Personal Data Breach Management & 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.

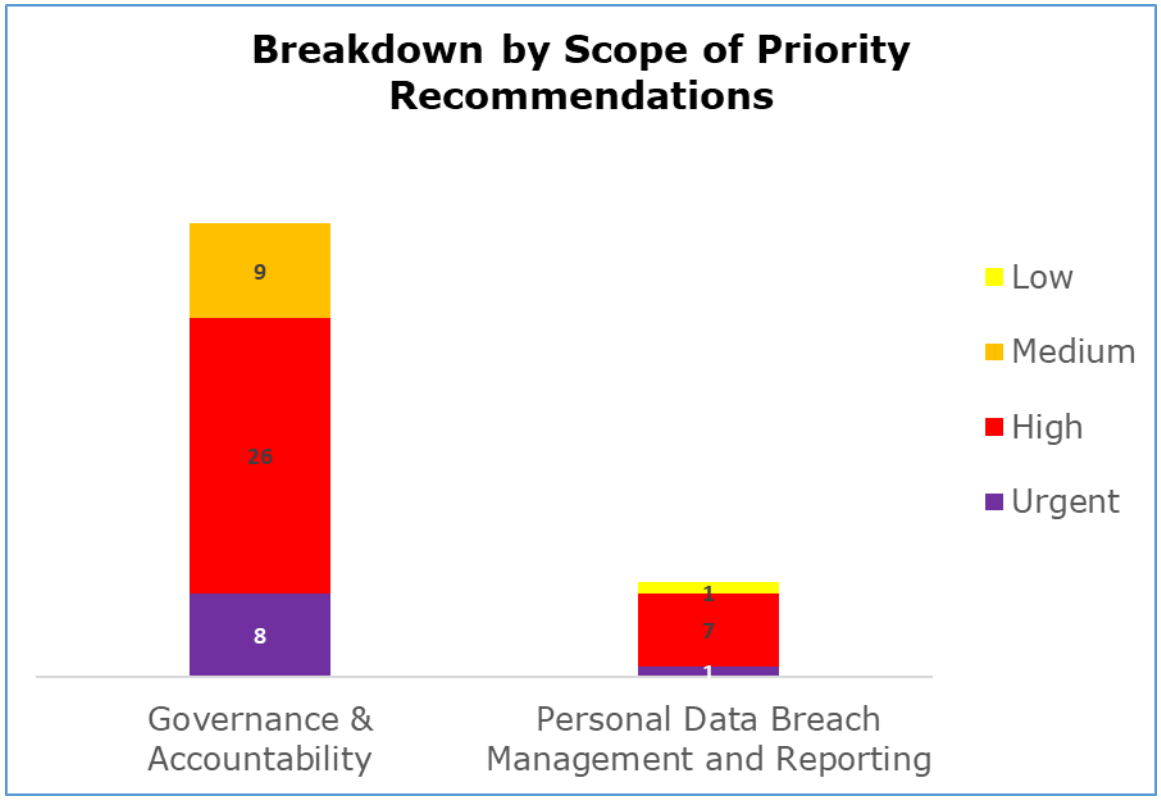
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist PSoS 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. PSoS'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	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.
Personal Data Breach Management & Reporting	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.

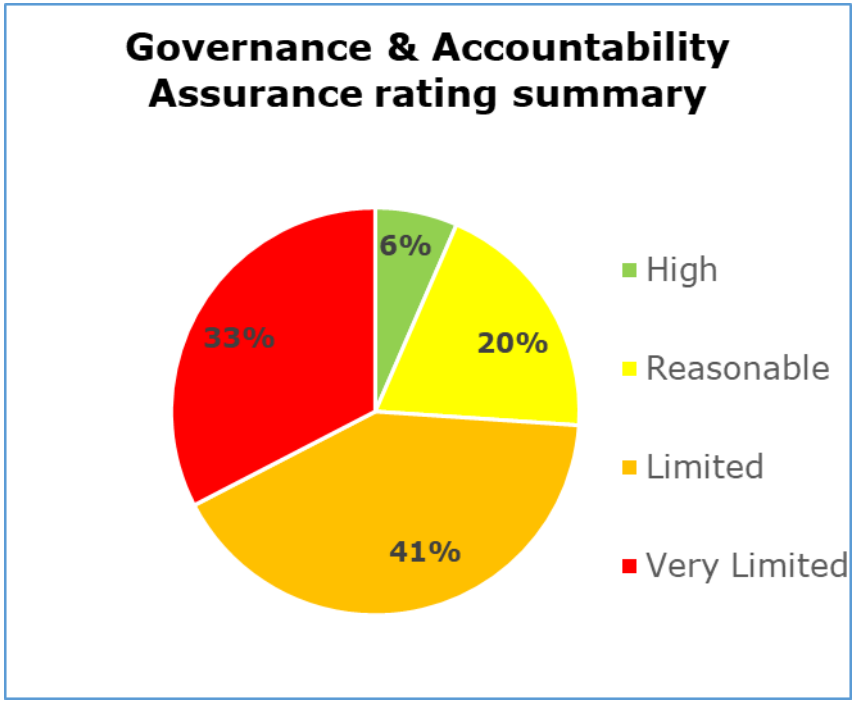
Priority Recommendations



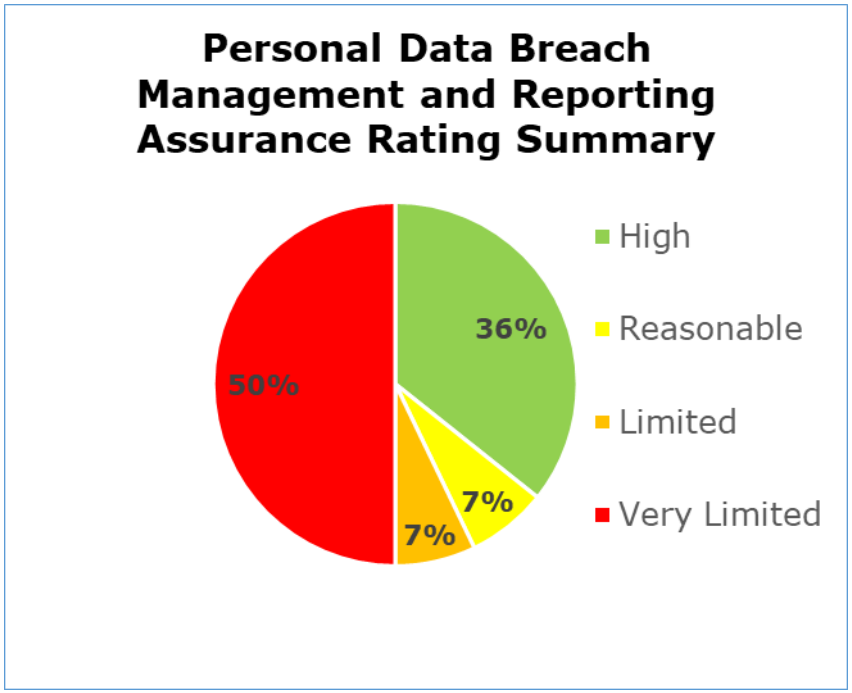
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has **8** urgent, **26** high, and **9** medium priority recommendations.
- Personal Data Breach Management & Reporting has **1** urgent, **7** high, and **1** low priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance & Accountability scope. **6%** high assurance, **20%** reasonable assurance, **41%** limited assurance, **33%** very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management & Reporting scope. **36%** high assurance, **7%** reasonable assurance, **7%** limited assurance, **50%** very limited assurance.

Areas for Improvement

PSoS should review their data mapping, ensuring their Information Asset Register (IAR) remains accurate. PSoS should then use the information gathered to create a Record of Processing Activities (RoPA) which meets the requirements set out in s.61 of the DPA18.

Clarity around the use of consent as a lawful basis under Data Protection (DP) legislation throughout the organisation, and a clear process for determining and recording the appropriate lawful basis for all data processing.

Policies should be overarching and comprehensive to provide staff with sufficient details on DP requirements. Policies should include how compliance will be monitored, with compliance checks in place to ensure staff have read and understood policies and procedures and are adhering to them.

A programme of both internal and external audits relating to DP should be implemented to provide assurance of the effectiveness of PSoS's controls and processes.

PSoS should ensure that privacy information is regularly reviewed, and create accessible versions of privacy notices for children, vulnerable adults, and individuals who require a language other than English.

Expand training modules to include role-specific training for staff with responsibilities for handling SARs and PDBs.

PSoS should continue working towards ensuring that there are measures in place for all systems to allow monitoring of inappropriate access and, or disclosure of personal data, in order to meet the requirements set out in DPA18 s.62 by the 2026 deadline.

PSoS should ensure that the Data Protection Officer (DPO) has sufficient resources to carry out their role effectively and independently. Their training should be updated to remain knowledgeable of any big legislative changes, and they should monitor compliance with and awareness of DP legislation. The DPO should also be involved in the DPIA process and data breaches.

Whilst PSoS have some processes in place for reporting PDBs, these should be appropriately approved and documented. The currently used process needs to be reviewed, amended and formalised with corresponding guidance created. This should include internal reporting processes, as well as those for reporting breaches to the ICO and to data subjects.

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 PSoS.

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