Scottish Courts and Tribunals Service

Data protection audit report

August 2025

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.

The Scottish Courts and Tribunals Service (SCTS) agreed to a consensual audit of its data protection practices.

The purpose of the audit is to provide the Information Commissioner and SCTS with an independent assurance of the extent to which SCTS, 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 SCTS's processing of personal data. The scope may take into account any data protection issues or risks which are specific to SCTS, identified from ICO intelligence or SCTS'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 SCTS, the nature and extent of SCTS's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to SCTS.

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 to both the UK GDPR and national data protection legislation are in place and in operation throughout 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.

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 SCTS in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to

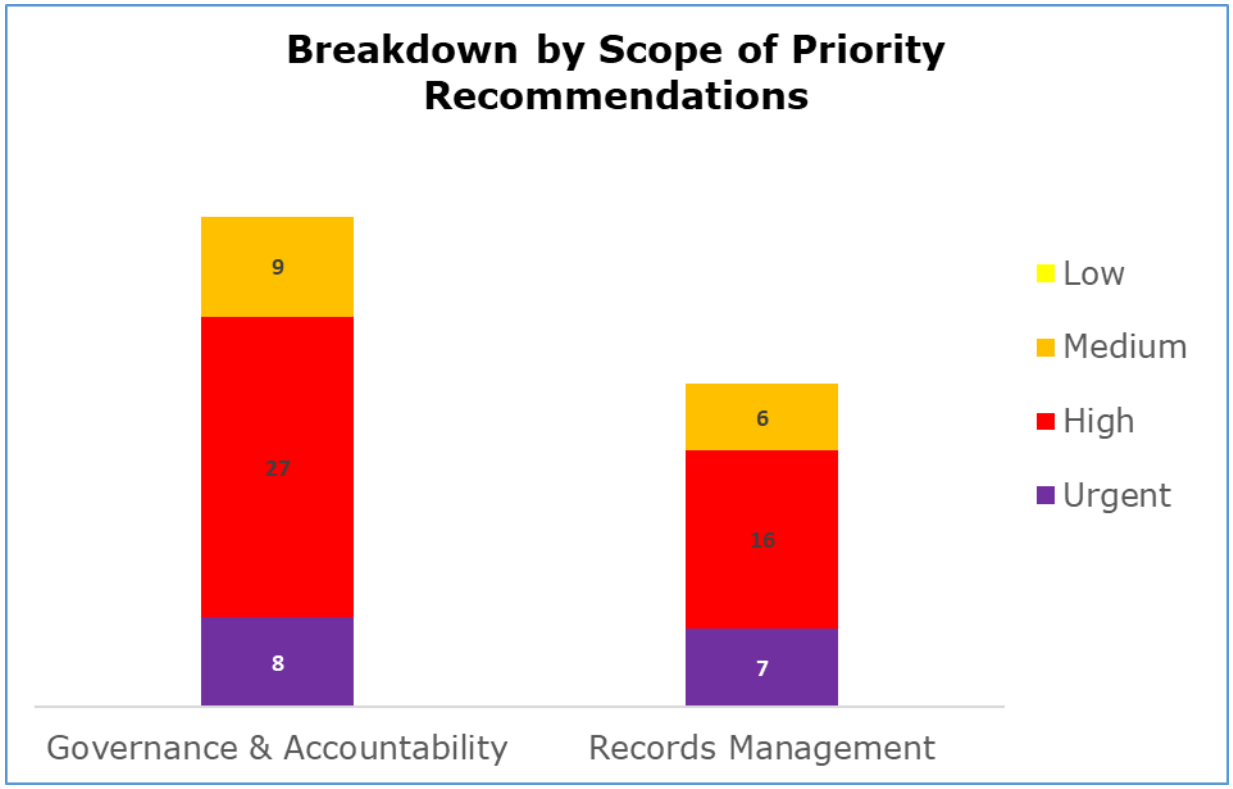
address. The ratings are assigned based upon the ICO's assessment of the risks involved. SCTS's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating*	Overall Opinion
Governance and Accountability	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.
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.

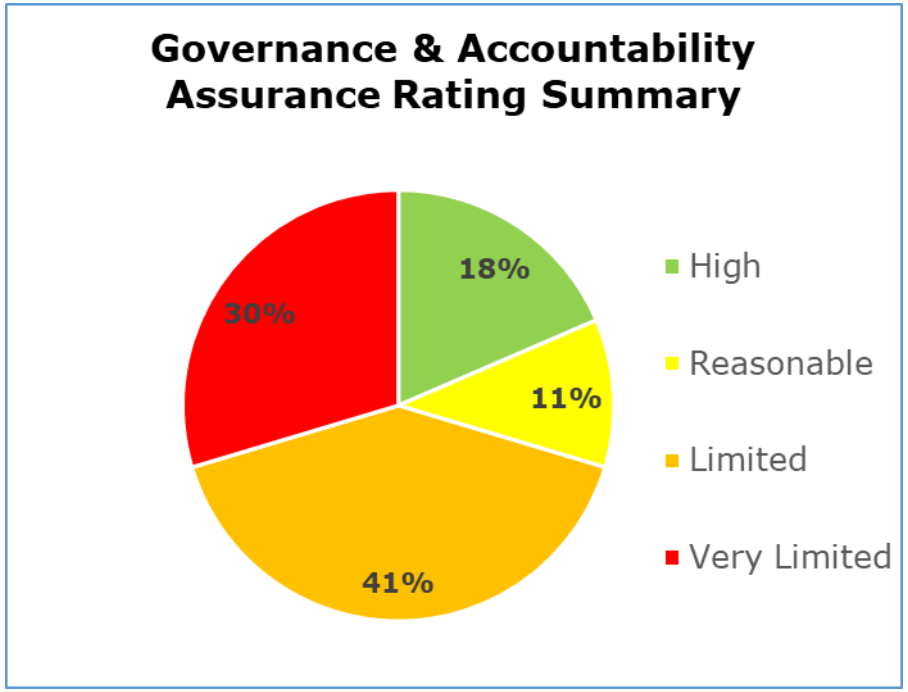
*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

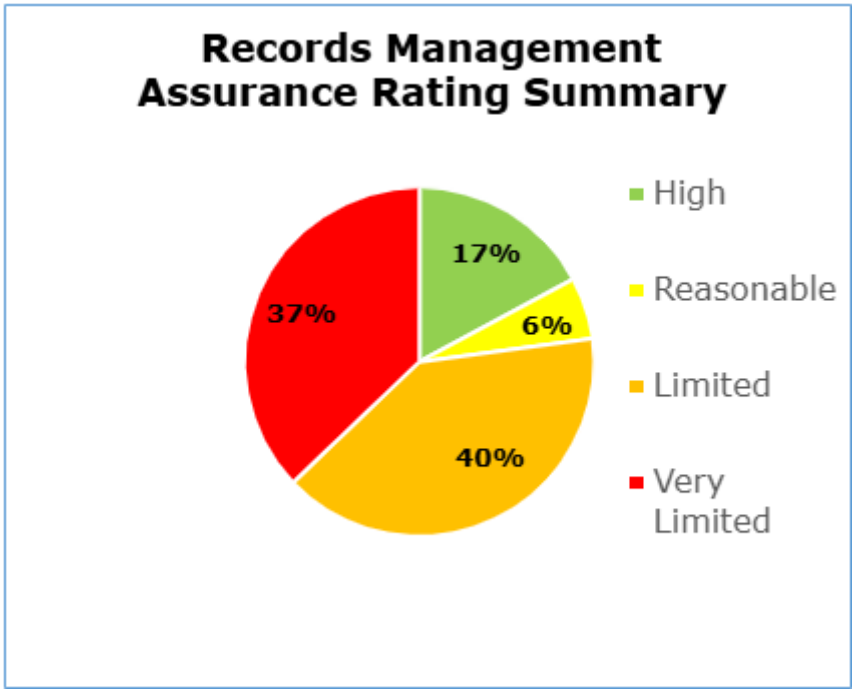


- Governance and Accountability has eight urgent, 27 high, and nine medium priority recommendations.
- Records Management has seven urgent, 16 high, and six medium priority recommendations.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 18% high assurance, 11% reasonable assurance, 41% limited assurance, 30% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 17% high assurance, 6% reasonable assurance, 40% limited assurance, 37% very limited assurance.

Key areas for improvement

We identified some key areas within our audit, where SCTS needed to implement further measures to fully comply with data protection law.

Governance and Accountability

- Policies and procedures regarding data protection (DP) and information governance (IG), must be reviewed regularly and kept up to date. This includes any privacy notices (PN), which detail how SCTS processes personal information.
- Implement a Record Of Processing Activity (ROPA) based on a comprehensive data mapping exercise and ensure it meets the legislative requirements within the UKGDPR and DPA18. Ensure this clearly captures the lawful bases and conditions relied on for processing in every business unit.
- Ensure that there is consistent central oversight of all DP practices throughout every business unit in SCTS.

Records Management

- Continue work reviewing or creating a suite of policies and processes around Records Management (RM). Once these documents are approved, SCTS should ensure they are effectively communicated, implemented and monitored.
- Conduct a survey audit of its paper records, to assess potential risks in storage caused by resourcing issues and the National Records Scotland (NRS) being unable to transfer files to its archives.
- Work with NRS to ensure that retention schedules capture all records.

Key areas of assurance

At the time of the audit and based on the evidence seen by auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

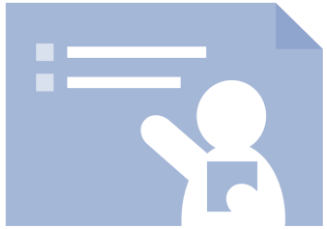
Governance and Accountability

- Awareness of staff around the Data Protection Impact Assessment (DPIA) process and the use of pre-screening checklists are well embedded across the organisation.
- There is a good provision of external audit in use by SCTS.

Records Management

- There was evidence of audits carried out to assess the security of inhouse records by both SCTS and NRS.
- Access to electronic files is controlled based on what is required for staff to fulfil their roles and these accesses are reviewed regularly, including inactive accounts.

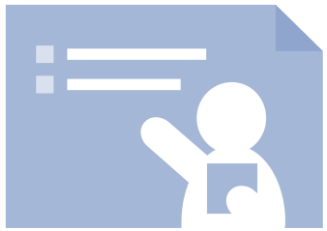
Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits



ICO Audit Team

ICO Team Manager – Grace Morgan
ICO Engagement Lead Auditor – Corey Davies
ICO Lead Auditors – Katy Wyton, Patrick Mitchell

Thanks

The ICO would like to thank Nicola Anderson - Director of Legislation and Information Unit and Leanne Jobling - Head of Information Governance and Correspondence Team for their help in the audit engagement.

Distribution List

This report is for the attention of Malcom Graham – Chief Executive, Nicola Anderson - Director of Legislation and Information Unit, and Leanne Jobling - Head of Information Governance and Correspondence Team.

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 Scottish Courts and Tribunals Service.

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