NHS National Services Scotland

Data protection audit report

July 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.

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

It was agreed that the audit would focus on the following areas

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.
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.
Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the organisation.

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.

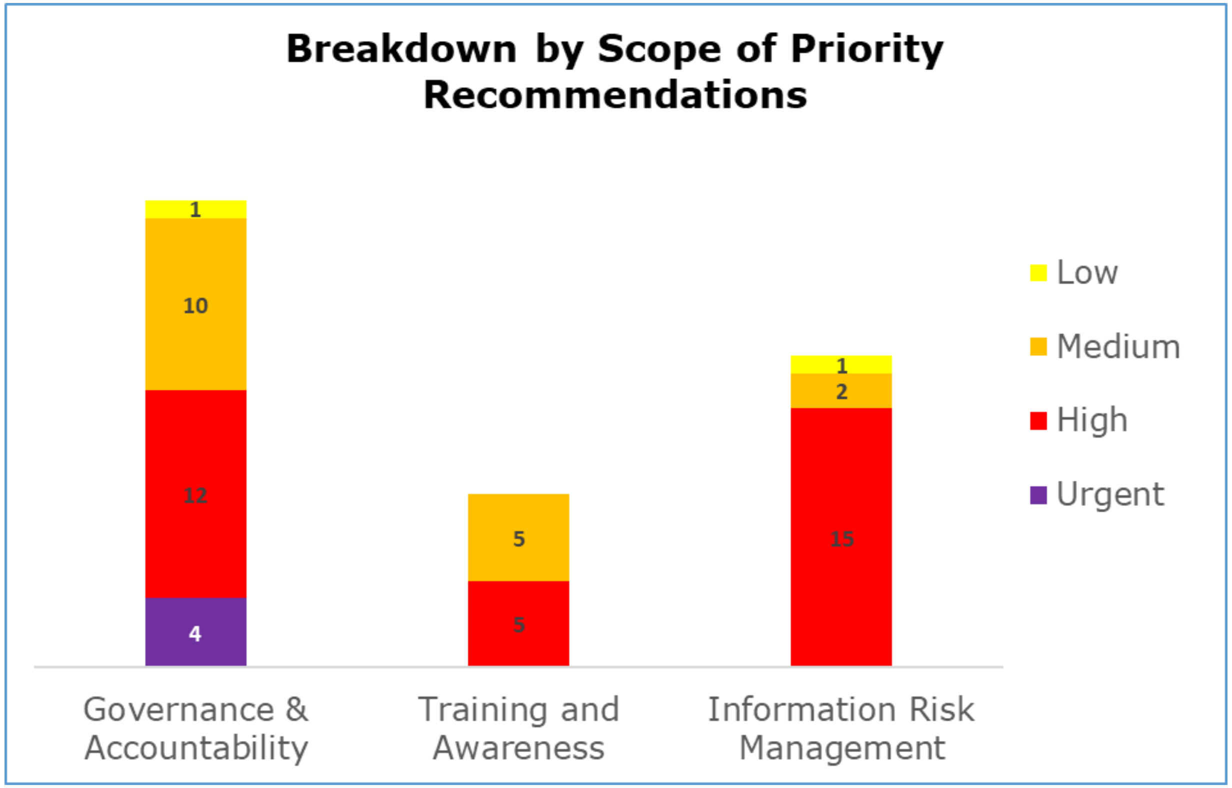
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist NHS NSS in implementing the recommendations each has been assigned a priority rating based upon the risks that they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

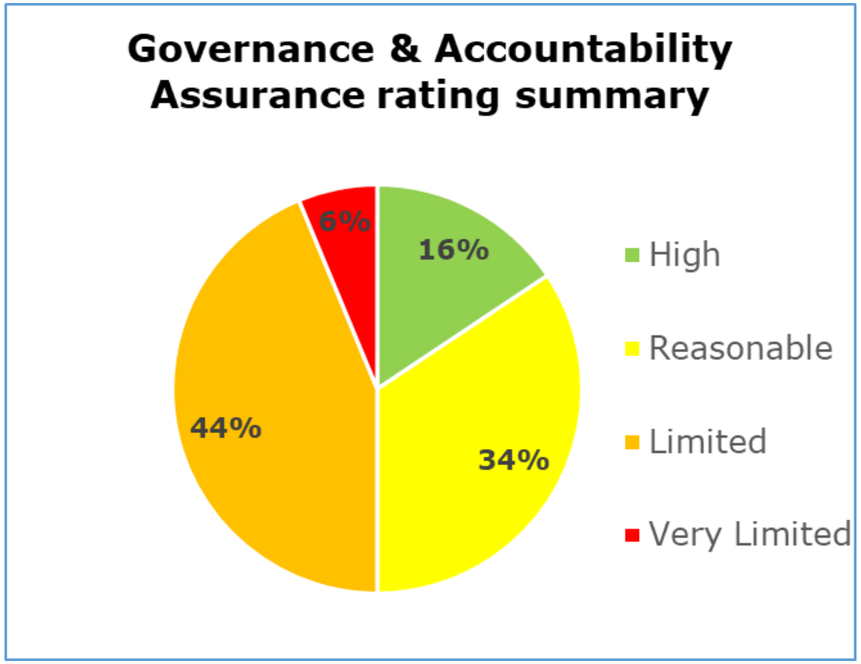
Priority Recommendations



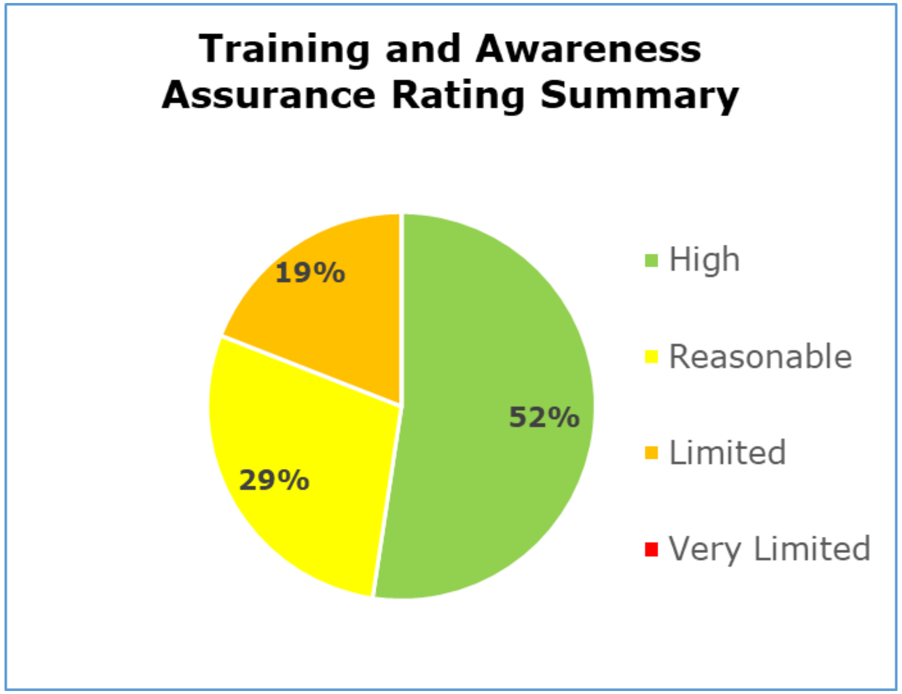
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 4 urgent, 12 high, 10 medium and 1 low priority recommendations.
- Training and Awareness has 0 urgent, 5 high, 5 medium and 0 low priority recommendations.
- Information Risk Management has 0 urgent, 15 high, 2 medium and 1 low priority recommendations.

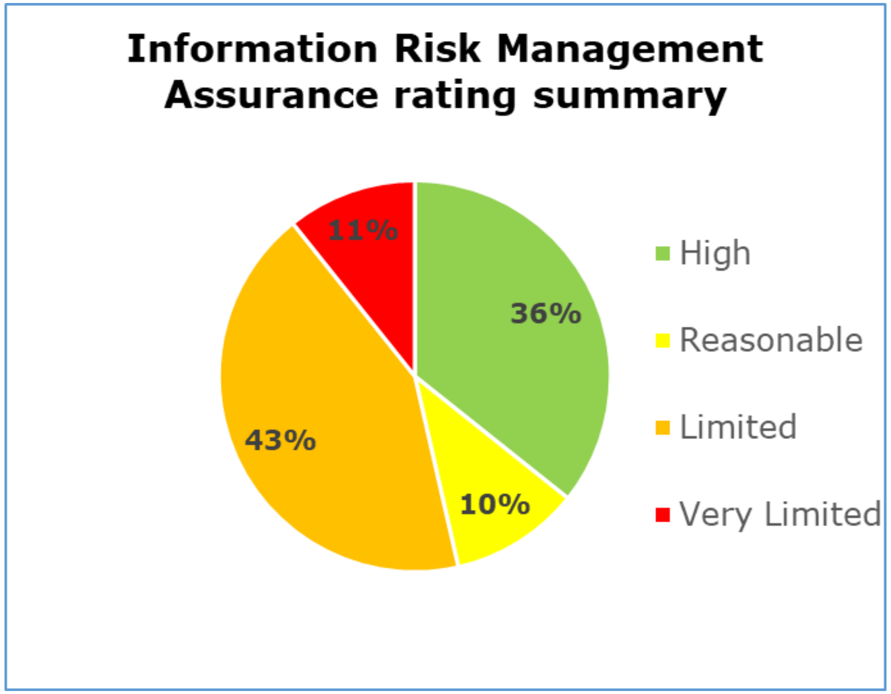
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 16% high assurance, 34% reasonable assurance, 44% limited assurance, 6% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Training and Awareness scope. 52% high assurance, 29% reasonable assurance, 19% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 36% high assurance, 10% reasonable assurance, 43% limited assurance, 11% very limited assurance.

Areas for Improvement

Governance and Accountability:

- NHS NSS is unable to demonstrate that it has a clear understanding of its current data flows, which means that its existing directorate-level and corporate Records of Processing Activities (ROPAs) may be based on inaccurate or incomplete information. NHS NSS has told the ICO that work is scheduled to commence in H2 2023 to carry out a comprehensive data flow mapping exercise. The outputs from this exercise should be the starting point for the development of NHS NSS's ROPA which, when complete, should be regularly reviewed to ensure that it remains accurate, up to date and meets UK GDPR Article 30 requirements.

- NHS NSS does not have a programme of risk-based internal information governance/data protection (IG/DP) audits in place to assess and monitor its compliance in this area. In the absence of such a programme, NHS NSS can have no assurance that its IG/DP risk management and compliance is effective.

- There is an opportunity to develop the range of Key Performance Indicators (KPIs) that are produced to ensure that all areas of IG/DP compliance and performance are being monitored. The frequency and format that IG/DP KPIs are reported to internal stakeholders, including senior management, should be improved to provide more effective oversight of performance in this area, and to help ensure that any decisions concerning IG/DP are supported by clear and timely metrics.

- A number of NHS NSS's IG/DP policies and procedures are beyond their scheduled review date and there are also gaps in the current IG/DP policy framework. For example, there is no Data Sharing Policy in place to document NHS NSS's approach to sharing personal data with other data controllers both on a routine and ad hoc basis.

Training and Awareness:

- The frequency of mandatory information governance refresher should be increased to provide staff with sufficient and up-to-date knowledge around data protection issues and therefore reduce the risk of data breaches due to a lack of current knowledge.

- A comprehensive training needs analysis around information governance training needs to be undertaken to enable the identification of all staff who require specialist information governance training in addition to the standard mandatory training and appropriate training provided regularly.

- The Information Security and Governance Group should improve its oversight of Information governance training compliance by including review of training completion figures as part of its regular meetings.

Information Risk Management:

- There should be measures in place to ensure that any risks identified in the course of the DPIA process are incorporated into appropriate risk registers, work plans or action plans, and then managed in accordance with the information risk management procedures.

- Before any processing takes place, NHS NSS should ensure that the DPIA has been completed and approved, and that evidence has been recorded of mitigating controls which are in place and effective.

- There should be a procedure for information assets to have a periodic risk assessment that is regularly reviewed and updated, so that risks are documented, managed and effectively mitigated.

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 NHS NSS.

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