Lewisham and Greenwich NHS Trust

Data Protection and Freedom of Information audit report

November 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 (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 purpose of the audit is to provide the Information Commissioner and Lewisham and Greenwich NHS Trust (the Trust) with an independent assurance of the extent to which the Trust, within the scope of this agreed audit, is complying with data protection and freedom of information legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Trust's processing of personal data and compliance with the Freedom of Information Act 2000 (FOI). The scope may take into account any data protection issues or risks which are specific to the Trust, identified from ICO intelligence or the Trust'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 the Trust, the nature and extent of the Trust's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the Trust.

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

Scope area	Description
Cyber Security	The extent to which the organisation has technical and organisational measures in place to protect personal data from external and internal attacks on confidentiality, integrity and availability.
Freedom of Information (FOI)	The extent to which FOI/Environmental Information Regulations (EIR)accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

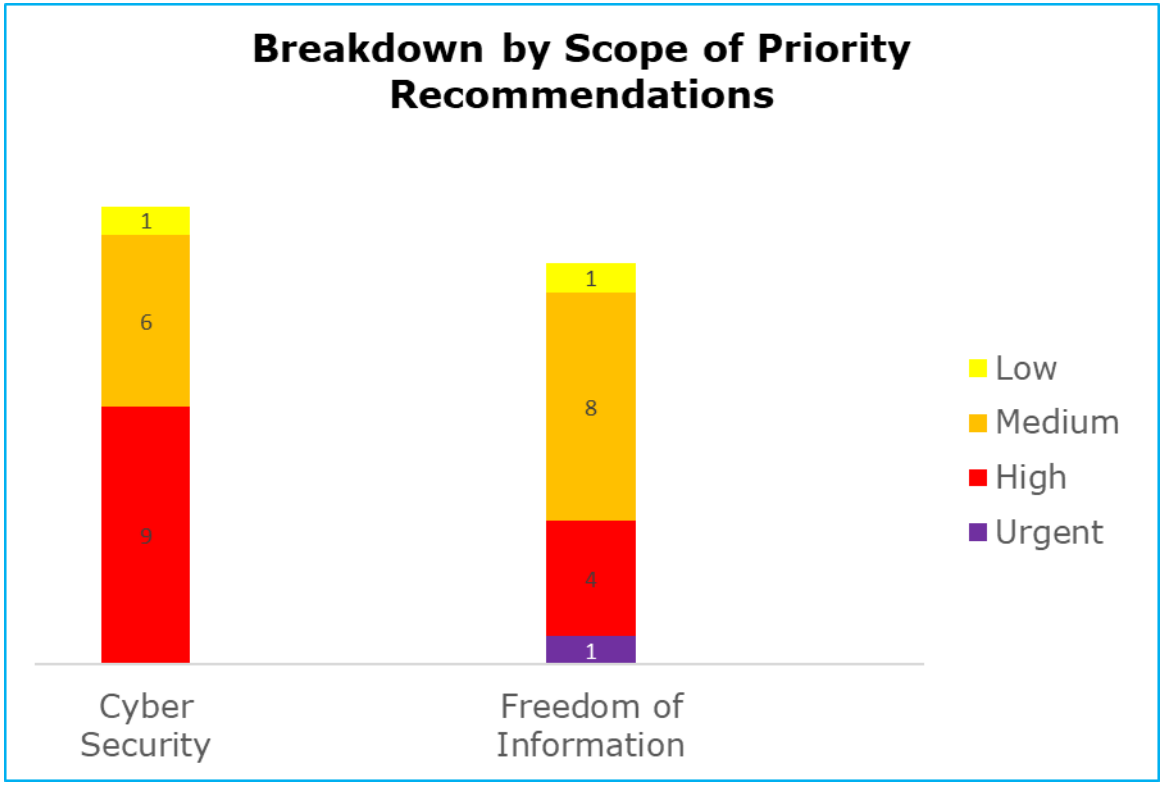
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential 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 the Trust 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. the Trust'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
Cyber Security	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.
Freedom of Information	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

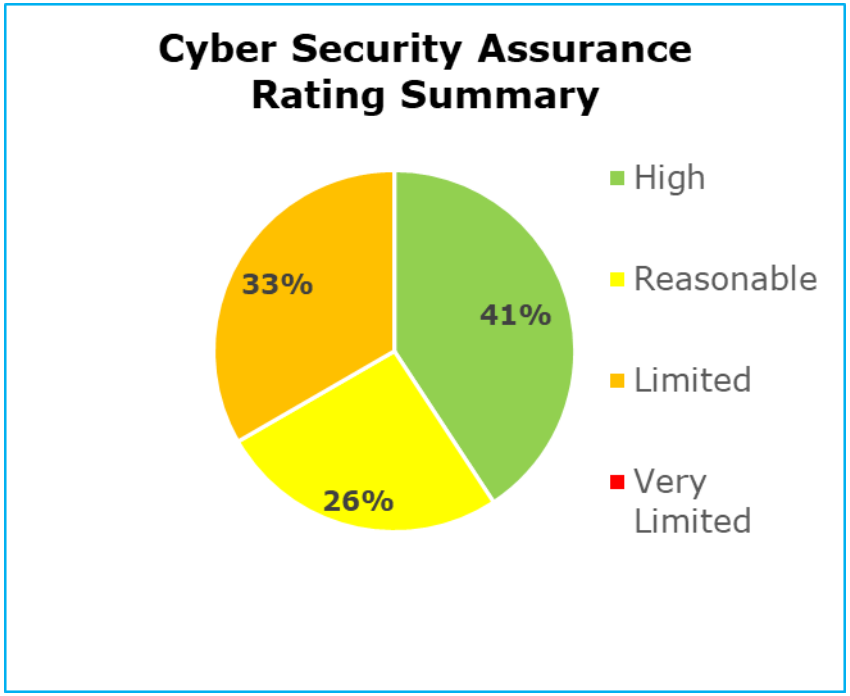
Priority Recommendations



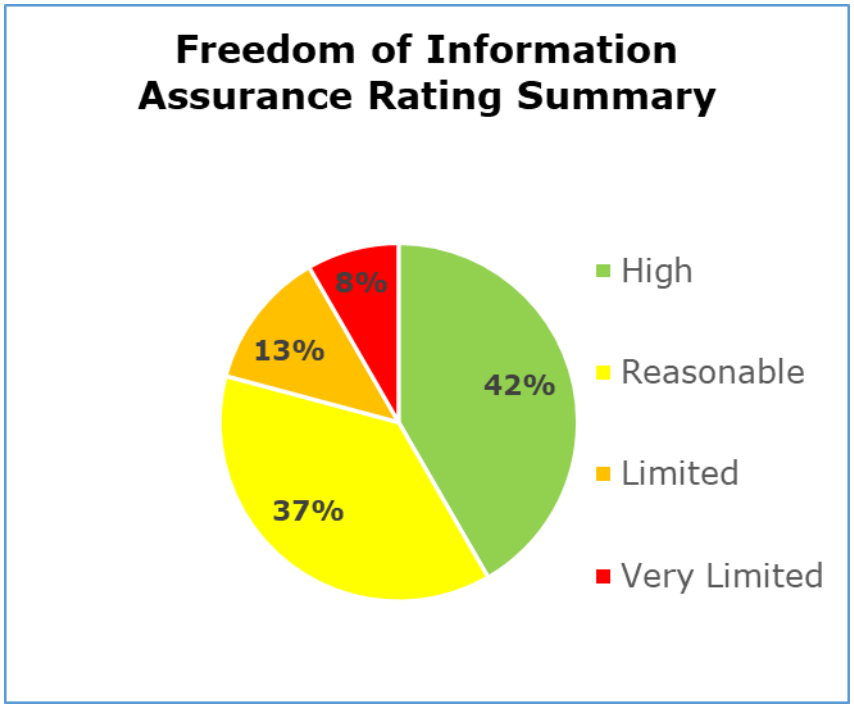
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Cyber Security has 9 high, 6 medium and 1 low priority recommendations.
- Freedom of Information has 1 urgent, 4 high, 8 medium and 1 low priority recommendations.

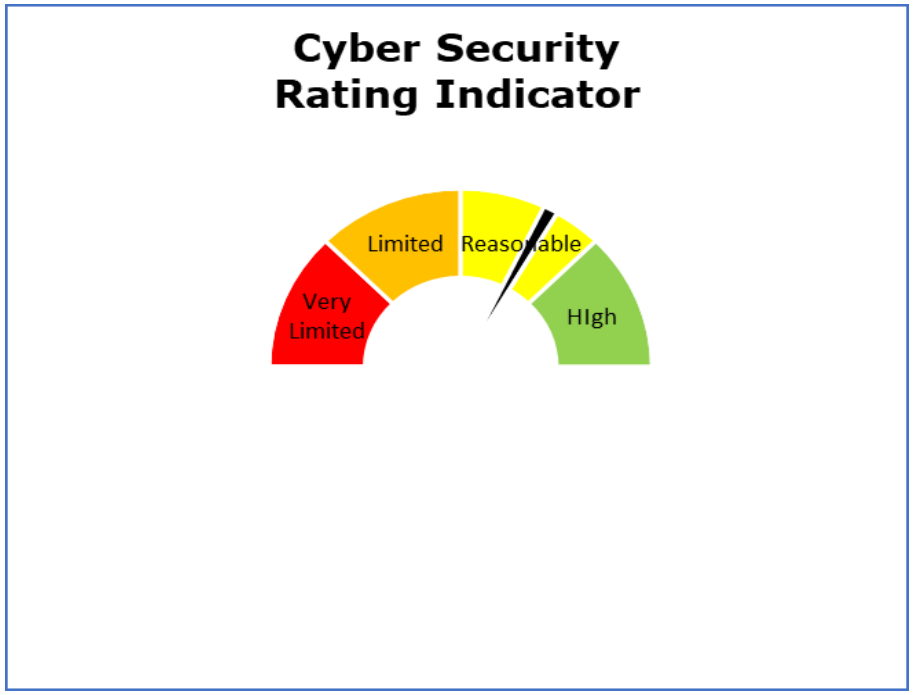
Graphs and Charts

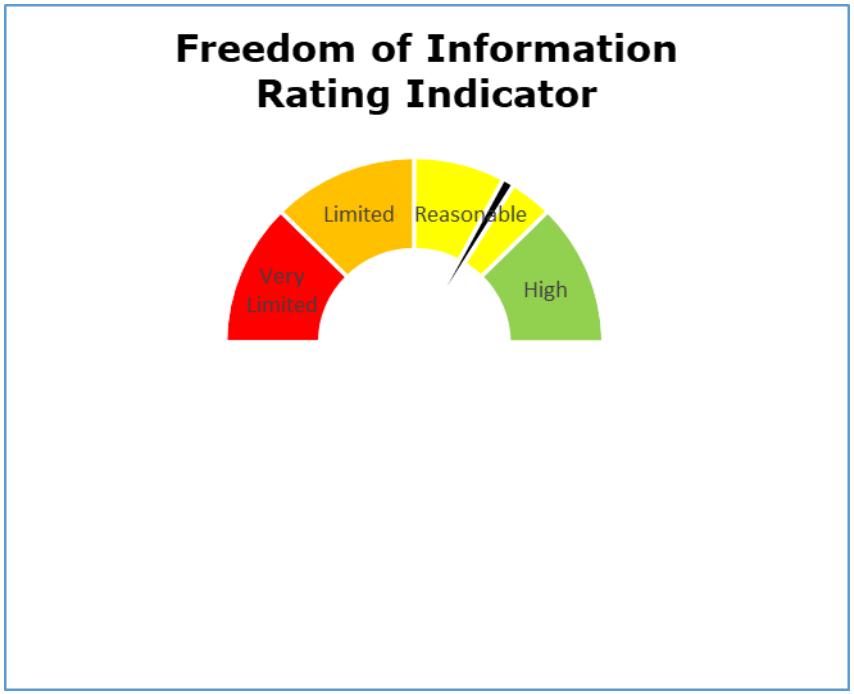


The pie chart above shows a summary of the assurance ratings awarded in the Cyber Security scope. 41% high assurance, 26% reasonable assurance, 33% limited assurance, no very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 42% high assurance, 37% reasonable assurance, 13% limited assurance, 8% very limited assurance.





The speedometer chart above gives a gauge of where the Trust sits on our assurance rating scale from high assurance to very limited assurance.

Areas for Improvement

Cyber Security

The cyber security framework should be further embedded, by integrating new cyber staff roles into the organisation, finalising the Trust cyber security strategy, and ensuring staff with key cyber security responsibilities complete additional specialised training relevant to their responsibilities. This should be supported by continuing work to improve security controls in place, such as plans to implement multi-factor authentication to protect higher risk or more sensitive personal data processing activities, and a regular programme of practical social engineering or phishing tests to ensure staff are familiar with such scams and what action to take.

Cyber risks relating to third party suppliers should be meaningfully reviewed periodically to ensure the Trust has assurance that cyber security controls are in place and effective. Further to this, Data Protection Impact Assessments should identify cyber risks and mitigating controls. Additionally, Information Asset Owners should be actively involved in assessing the cyber risks and monitoring the effectiveness of the mitigating controls relating to their information assets.

Ongoing work to replace or decommission legacy devices that cannot receive security patches and phase out or update servers with unsupported operating systems should continue. Moving forward, all network devices should be able to receive security patches that address cyber vulnerabilities, and systems approaching end of life should be removed or updated in a timely manner to ensure these do not pose a significant cyber risk.

Freedom of Information

The Trust is not currently achieving the 90% target for compliance with the statutory timescale for FOI requests. In addition, there is an increasing trend in the volume of requests the Trust receives. The contributing factors affecting compliance rates in this area should be identified, and appropriate steps taken to improve.

The recent specialised training for the IG team should be regularly refreshed, and training records maintained and monitored. There are opportunities for the Trust to also improve the training it provides to all staff and to increase awareness of FOI across the organisation. This would help to ensure that staff are regularly reminded of the requirements under the Act and their obligations.

Communicating policies and procedures to staff should also be carried out via a formal process so that the Trust can be assured that staff are up to date with current guidance. This should include any policy or process updates.

Best Practice

The Trust has implemented a Change Advisory Board that reviews and approves all IT change projects before proceeding. All IT changes are subject to appropriate scrutiny including a review of rollback proposals, and actively monitored after implementation, which helps to give assurance that IT change management governance is effective.

The Trust has contracted an external penetration test supplier that is NCSC-approved and uses appropriate penetration testing methodologies under the CHECK scheme.

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 Lewisham and Greenwich NHS Trust.

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