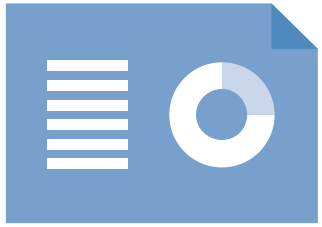
Central and North West London NHS Foundation Trust

Data protection audit report

June 2021

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 sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The purpose of the audit is to provide the Information Commissioner and Central and North West London NHS Foundation 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 legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Trust processing of personal data. 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 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 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
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 UKUK GDPR and national data protection legislation are in place and in operation throughout the organisation.
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.

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

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore the Trust agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 26 April to 30 April 2021 The ICO would like to thank the Trust for its flexibility and commitment to the audit during difficult and challenging circumstances.

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.

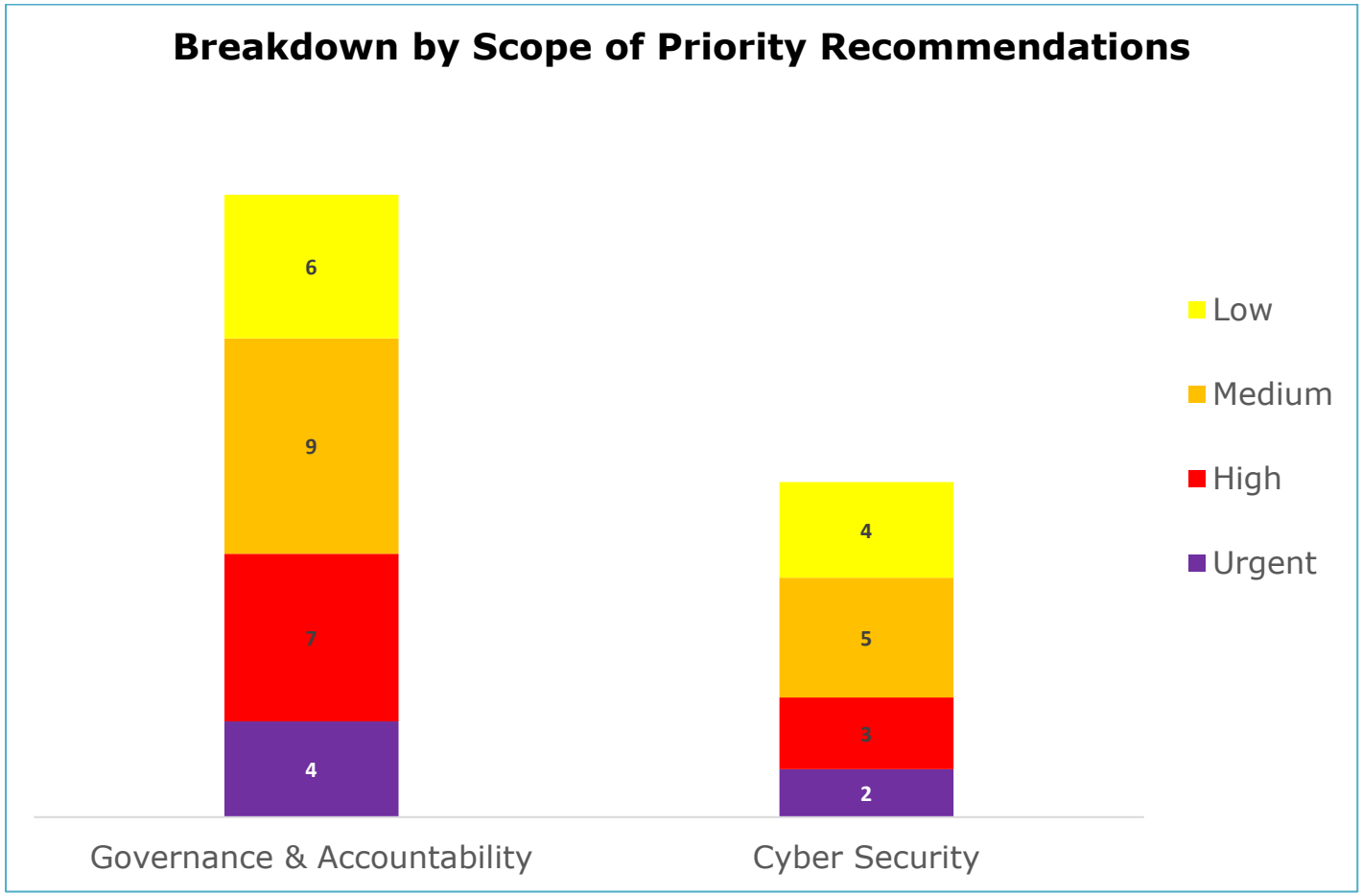
The ratings are assigned based upon the ICO's assessment of the risks involved. The Trust's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

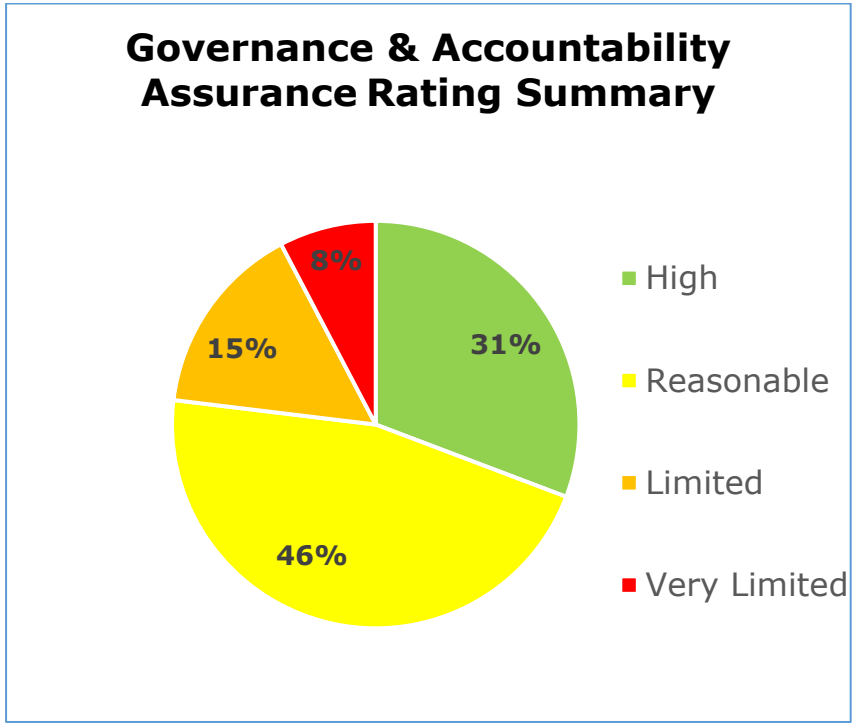
Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
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.

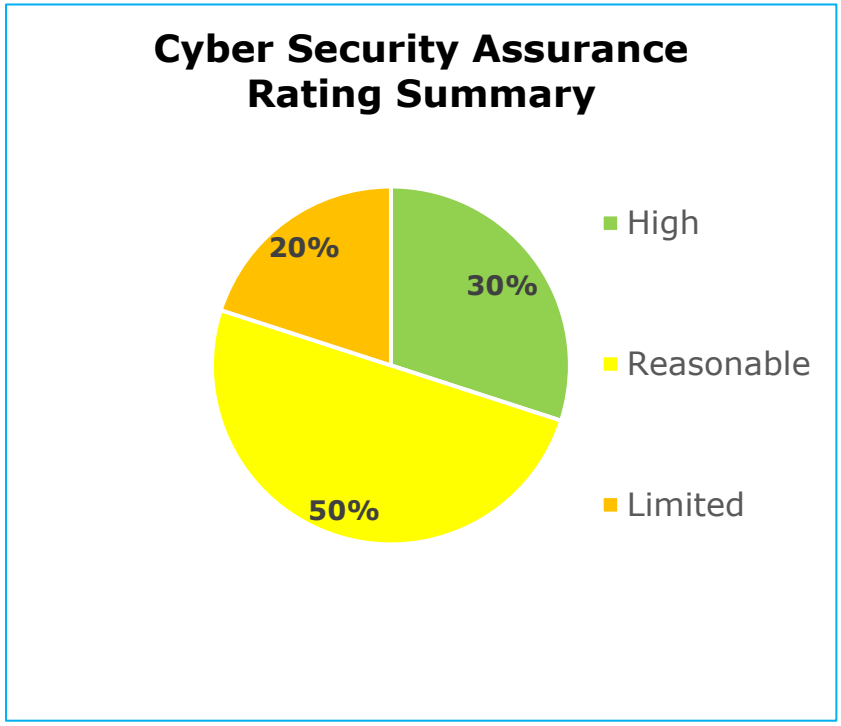
**The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.*

Priority Recommendations



Graphs and Charts





Areas for Improvement

Governance and Accountability

- The recording of data processing activities within the Trust needs improvement. A comprehensive data mapping exercise should be undertaken, and a formal Record of Processing Activity (ROPA) created, which conforms to all the requirements set out in Article 30 of the UK GDPR.

- The provision of privacy information on the Trust's public website requires improvement, as there are currently two sections where privacy information is carried, a page called 'Your information' and a separate 'Fair Processing Notice'. Although they cover some of the same areas, there are some sections included on one but not the other, which could prevent data subjects finding all the information required in privacy information under Articles 13 and 14 of the UK GDPR. Furthermore, the correct information regarding how to make a subject access request should be available on the website for data subjects.

- The Information Governance structure in the Trust requires strengthening to provide assurance that the DPO is able to carry out their role in an appropriately effective manner as required by data protection legislation.

Cyber Security

- Awareness needs to be raised among staff of social engineering and the risk it can pose to the protection of personal data and cyber security. In addition, there is a lack of awareness of what staff are expected to do in the event that they fall victim to a suspected social engineering attack.

- Mobile device management should be improved, as it is possible for staff to download instant messenger apps onto a Trust mobile device, and there is also limited oversight of which members of staff have access to and are using instant messenger apps.

Best Practice

There is a Privacy by Design Policy in force which helps reinforce the culture of privacy awareness within the 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 Central and North West London NHS Foundation Trust (the 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 the Trust. The scope areas and controls covered by the audit have been tailored to the Trust, and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.