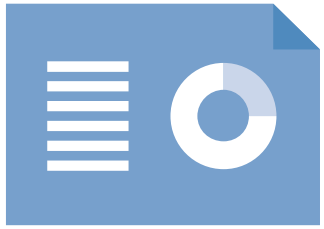
Guy's and St Thomas' NHS Foundation Trust

Data protection audit report

February 2020

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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.

Guy's and St Thomas' NHS Foundation Trust (GSTT) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 10 September 2019 with representatives of GSTT to discuss the scope of the audit.

Telephone interviews were conducted on prior to the onsite visit. The audit fieldwork was undertaken at GSTT sites in London on 21 – 23 January 2020.

The purpose of the audit is to provide the Information Commissioner GSTT with an independent assurance of the extent to which GSTT, within the scope of this agreed audit, is complying with data protection legislation.

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

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.
Business Continuity and Disaster Management	The extent to which the organisation has measures in place to ensure that personal data and data subjects are not adversely affected in the event of significant functional impacts on the organisation.
Personal Data Breach Management and 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.

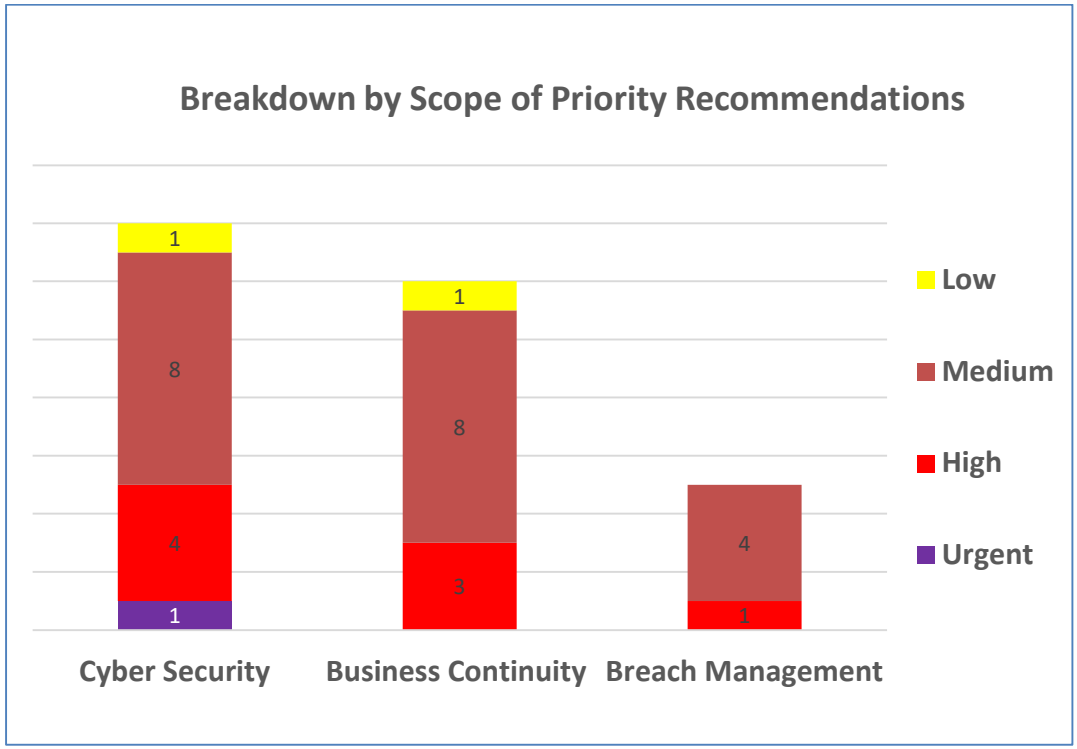
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist GSTT 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. GSTT'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.
Business Continuity	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.
Personal Data Breach Management	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

Priority Recommendations



Areas for Improvement

Cyber Security

GSTT should ensure key cybersecurity policies and practices are reviewed in line with their review dates. They need to develop a policy governing secure software development that includes monitoring and auditing of standards.

GSTT should review its use of removeable media to ensure it is properly controlled and accounted for. An asset register detailing a full inventory of removable media in use and ownership should be maintained with regular checks to confirm accuracy.

GSTT should ensure the use of all mobile apps used within the Trust are accounted for and that in their usage they are complying with legislation and providing all end users with the appropriate privacy information at the point of usage.

Business Continuity and Disaster Recovery

GSTT should ensure that all change management projects follow a fully documented procedure, and that there is resilience built into the Change and Release Manager's role.

There should be an overarching Disaster Recovery Plan made available to staff in order to ensure that there is overarching control and oversight of managing significant incidents.

In order to ensure that all staff can recognise and report a significant event, GSTT should consider providing an annual refresher session of Business Continuity Training for all staff.

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 GSTT.

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