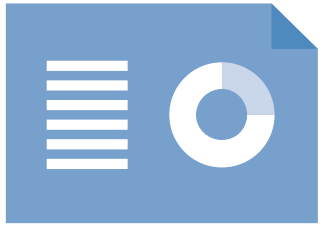
Cardiff and Vale University Health Board

Data protection audit report

September 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.

Cardiff and Vale University Health Board (Cardiff and Vale UHB) agreed to a consensual audit by the ICO of its processing of personal data.

Telephone interviews were conducted prior to the onsite visit. The audit fieldwork was undertaken at Cardiff and Vale UHB sites on 25 – 27 February 2020.

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

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 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.

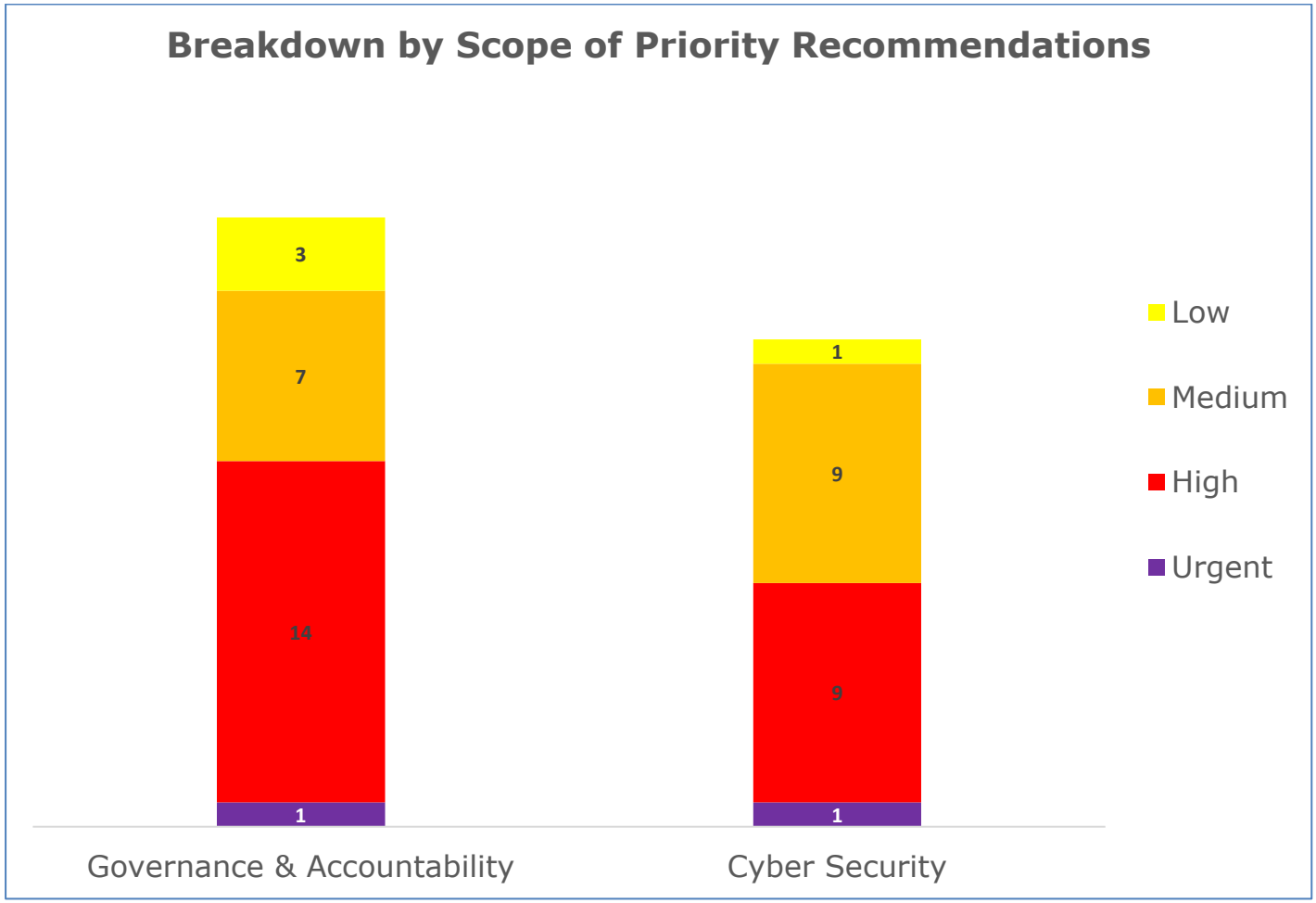
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist Cardiff and Vale UHB 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. Cardiff and Vale UHB 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 & 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.

Priority Recommendations



Areas for Improvement

Governance and Accountability

- Cardiff and Vale UHB need to ensure that there is no outdated privacy information on their website and that their Privacy Notice can be easily accessed by website visitors.

- There is no documented procedure to follow to ensure that individuals receive all required information when they are informed of a breach affecting their personal data.

- Cardiff and Vale UHB should ensure that all areas fully document their processing activities so they are aware of all information held and the flows of information within the organisation.

Cyber Security

- Cardiff and Vale UHB should put in place improvements in relation to cyber security training. The organisation's mandatory induction and refresher IG training has no cyber security components and frontline staff were not strong in their knowledge. Furthermore there are no Training Needs Assessments carried out for staff with security responsibilities.

- There are a number of gaps in the current policy structure. Several key polices are past their review date and therefore do not accurately or fully reflect current working practices across the variety of secure information systems the organisation deploys. There are also key policies missing in a number of areas.

- Cardiff and Vale UHB is generating and retaining a variety of logs for servers, workstations, and internet access however there isn't an overall logging policy in place.

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 Cardiff and Vale UHB.

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