Aneurin Bevan University Health Board

Data protection audit report

September 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.

Aneurin Bevan University Health Board (ABUHB) agreed to a consensual audit of its data protection practices.

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

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

Scope area	Description
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Requests for Access	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.
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, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential documentation.

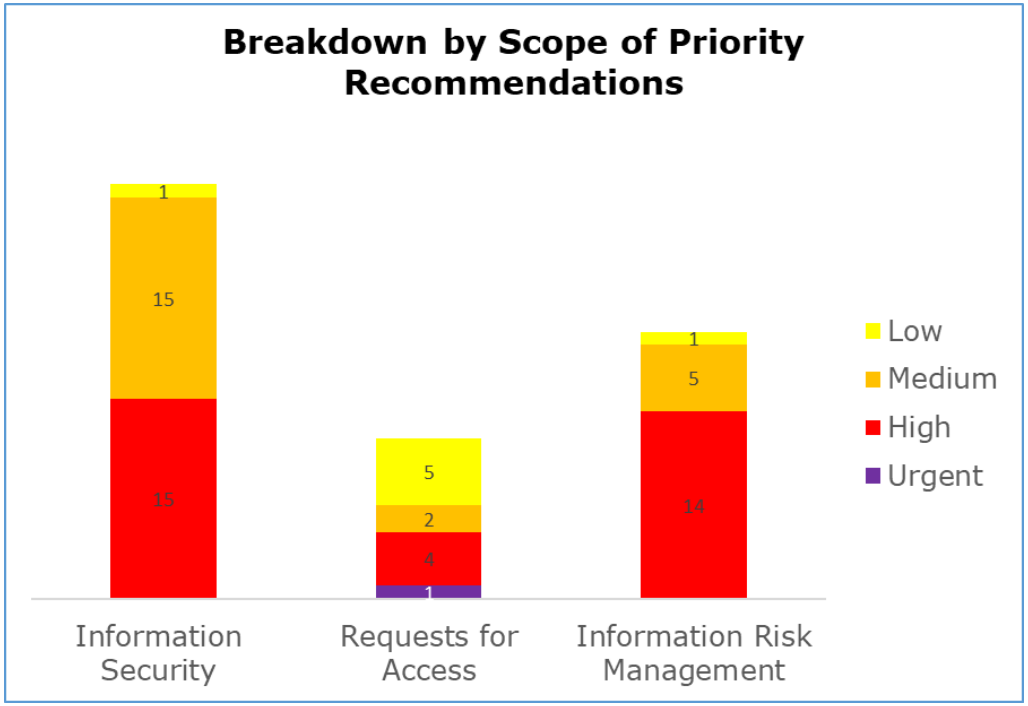
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist ABUHB in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address.

The ratings are assigned based upon the ICO's assessment of the risks involved. ABUHB'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
Information 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.
Requests For Access	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.

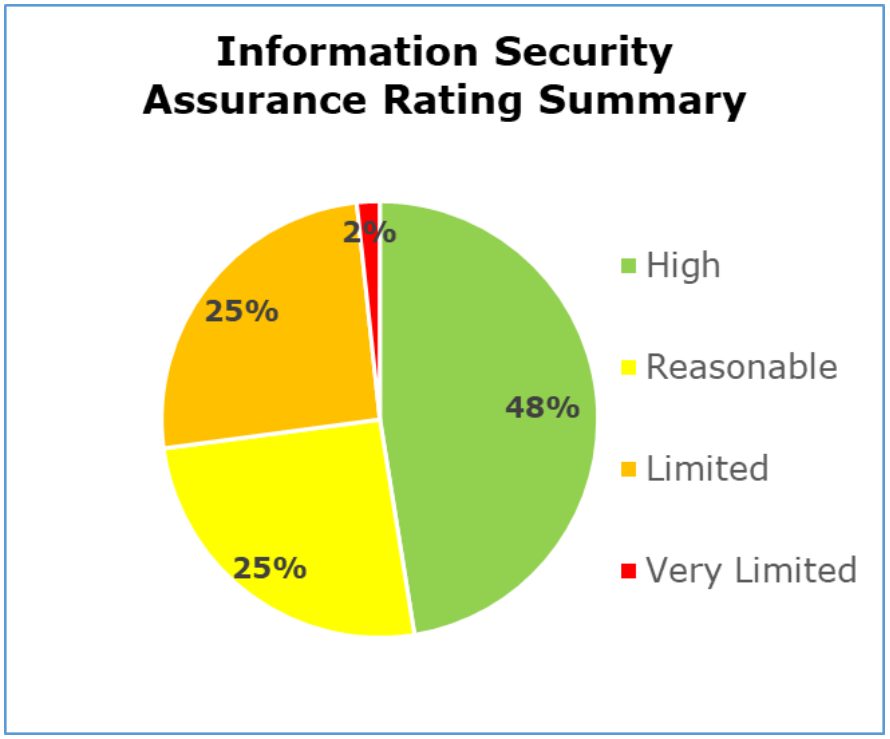
Priority Recommendations



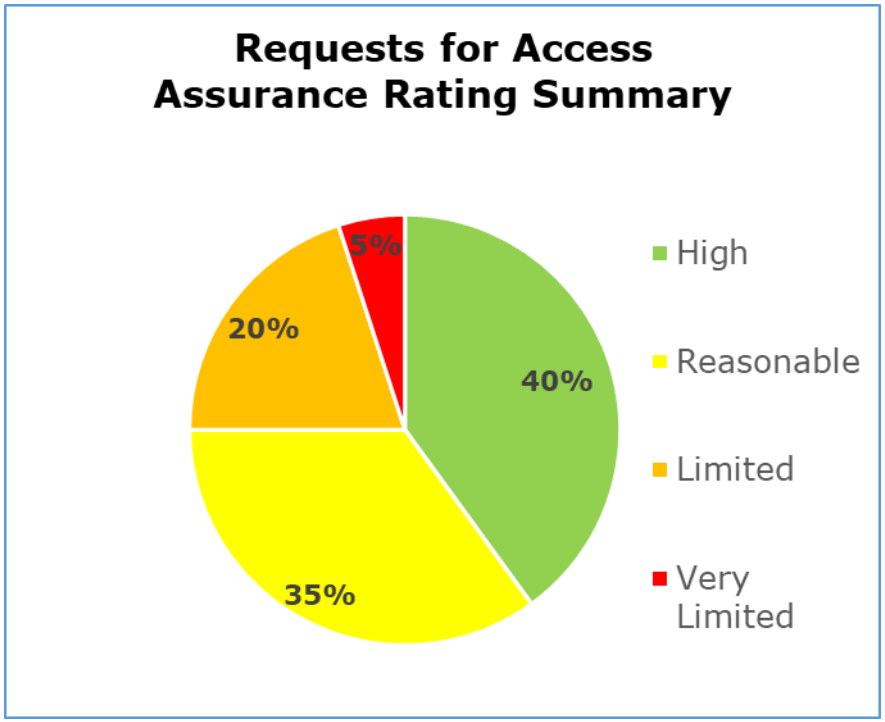
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- The Information Security scope area has no urgent, 15 high, 15 medium and one low priority recommendations.
- The Requests for Access scope area has one urgent, four high, two medium and five low priority recommendations.
- The Information Risk Management scope area has no urgent, 14 high, five medium and one low priority recommendations.

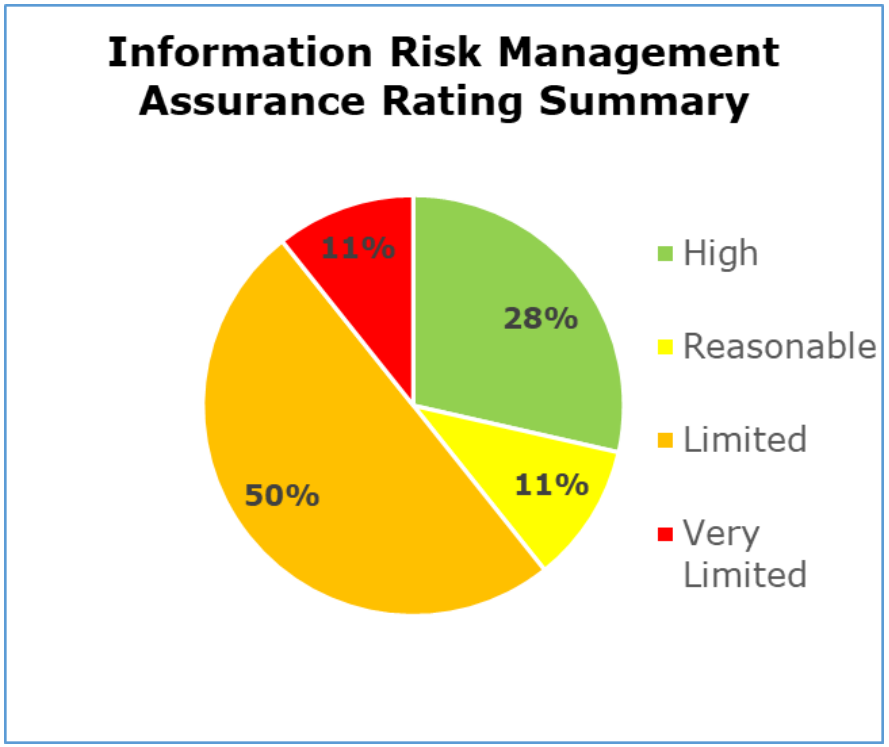
Graphs and Charts



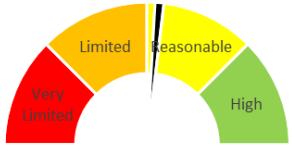
The pie chart above shows a summary of the assurance ratings awarded in the Information Security scope. 48% high assurance, 25% reasonable assurance, 25% limited assurance, 2% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Requests For Access scope. 40% high assurance, 35% reasonable assurance, 20% limited assurance, 5% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Risk Management scope. 28% high assurance, 11% reasonable assurance, 50% limited assurance, 11% very limited assurance.

Information Security Scope Rating Indicator	Requests For Access Scope Rating Indicator	Information Risk Management Scope Rating Indicator
		

The speedometer charts above gives a gauge of where ABUHB sits on our assurance rating scale from high assurance to very limited assurance for each scope area.

Areas for Improvement

Information Security

- ABUHB does not have a comprehensive organisational information security (IS) policy in place. A number of other policies and procedures that relate to IS and information risk are either in draft status and have not been published, are beyond their scheduled review date or do not contain adequate version/document control information.
- Compliance rates for mandatory information governance (IG) training, which incorporates elements of IS, is below ABUHB's target of 85%, and for some divisions and service areas the compliance rates are significantly lower. Where staff do not receive adequate IS training, there is an increased risk of IS incidents and personal data breaches. In addition, whilst there are good examples of IS awareness raising materials in place on ABUHB's intranet, audit interviews indicated there is work to do to ensure that all staff are aware of these materials and are working in a way that observes good IS practices and behaviours.
- Whilst a new IG governance structure is soon to be implemented, at the time of the ICO audit there was no central steering group in place to provide a forum for all relevant stakeholders to provide input on IS matters. As a result, ABUHB cannot have sufficient assurance that its approach to IS and the treatment of IS risks is effective.
- ABUHB's software and hardware asset registers are not subject to periodic review and risk assessment. Should the IS risks relating to different assets change over time, the controls in place to mitigate such risks may become outdated and ineffective.
- The process to review physical access rights requires improvement to provide assurance that staff and other individuals can only access the secure areas that they have a legitimate need to enter. There is also a need to implement improved controls around the use of 'generic' ID badges.
- Not all business continuity plans across ABUHB are currently subject to periodic testing at defined intervals or following significant changes to ABUHB's or the relevant service area's structure or set up.

- There is an opportunity to improve the frequency and type of internal and external IS reviews that are being undertaken to provide stronger assurance that IS controls have been implemented and are operating in accordance with ABUHB's documented policies and procedures.

Requests For Access

- ABUHB is not meeting the required timeframes for responding to requests for personal data in all cases. It is working towards improving its compliance, with the proposed introduction of a new case management system and new training for staff. ABUHB should continue with this work, and ensure that it monitors the effectiveness of measures implemented to improve the timeliness of its responses to subject access requests (SARs).
- In monitoring the above, ABUHB does not currently use key performance indicators (KPIs) and there are no formal reporting procedures for senior management to have oversight of the figures collected.
- ABUHB's SAR Policy is in draft status, and its SAR Standard Operating Procedure (SOP) is overdue for review. These documents should be included in ABUHB's programme of work to review, or add to, the published IG/DP policies and procedures it has in place.

Information Risk Management

- ABUHB does not have formalised processes in place for consultation with internal and external stakeholders during the Data Protection Impact Assessment (DPIA) process, and DPIAs do not always record comprehensive detail of any engagement.
- ABUHB undertakes reviews of DPIAs where there are changes to processing, however it does not have a formal schedule of regular reviews and DPIAs themselves do not include review dates.
- ABUHB does not currently undertake audits of DPIA controls, to ensure that they are effective in mitigating the risks required.

- ABUHB has not formally identified Information Asset Owners (IAOs), and staff who hold these responsibilities have not yet received sufficient training in all cases.
- As mentioned in the Information Security scope above, ABUHB has plans in place to introduce a new IG governance structure in which the SIRO will chair the Health Board Office of the SIRO (HBOTS). However, there are currently no formal reporting lines through which the SIRO receives reports on information risk management and DPIAs.
- ABUHB has departmental Information Asset Registers (IARs) which feed into an overarching IAR. However, the IARs do not currently capture sufficient information about information assets including review dates, retention periods and the associated risk.
- The risk register currently in use does not capture the mitigation measures decided for information assets, and no evidence was provided that appropriate action plans have been documented for all information risks that are designated to be treated or transferred.

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 Aneurin Bevan University Health Board.

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