Disclosure and Barring Service

Data protection audit report

May 2022

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 (UKGDPR), 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 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 Disclosure and Barring Service (DBS) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 27 January 2022 with representatives of DBS to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and DBS with an independent assurance of the extent to which DBS, 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 DBS processing of personal data. The scope may take into account any data protection issues or risks which are specific to DBS, identified from ICO intelligence or DBS's 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 DBS, the nature and extent of DBS's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to DBS. 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 UKGDPR and national data protection legislation are in place and in operation throughout the organisation.
Role of the DPO	The extent to which the organisation has complied with their obligations under UK GDPR to appoint an independent DPO who is properly trained and resourced.
Processor, Third Party Supplier and Controller Relationship Management	Organisations should ensure there are effective relationship management controls in place with all processors and 3rd party suppliers. Written contracts between controllers and processors are a requirement under the UKGDPR. These contracts must now include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the UKGDPR requirements, not just those related to keeping personal data secure.

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 DBS 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 28 March to 7 April 2022. The ICO would like to thank DBS for its flexibility and commitment to the audit during difficult and challenging circumstances.

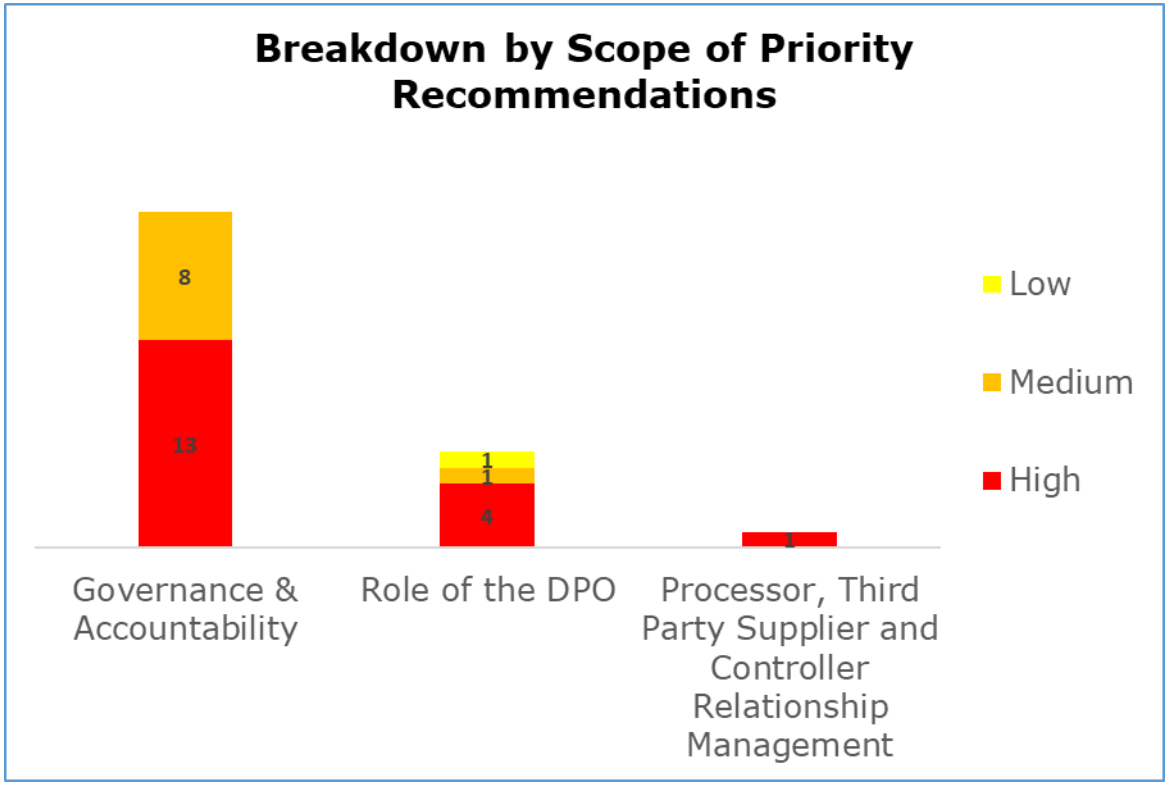
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist DBS in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. DBS'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.
Role of the DPO	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.
Processor, Third Party Supplier and Controller Relationship 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.

*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.

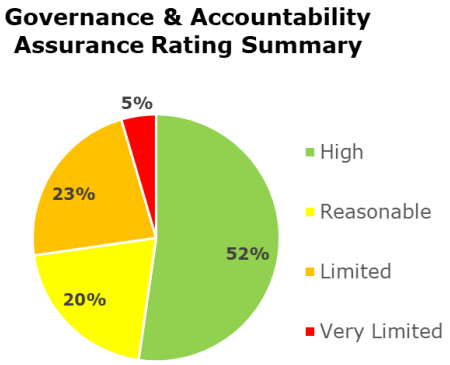
Priority Recommendations



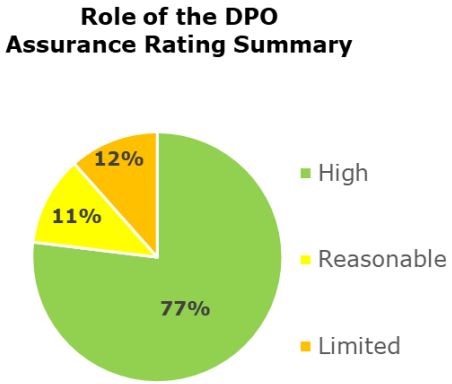
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 13 high and eight medium priority recommendations
- Role of the DPO has four high, one medium and one low priority recommendations
- Processor, Third Party Supplier and Controller Relationship Management has one high priority recommendation.

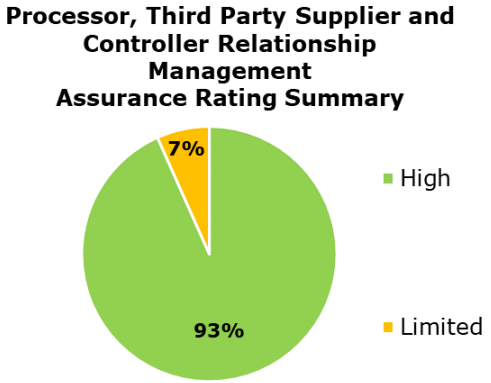
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 52% high assurance, 20% reasonable assurance, 23% limited assurance, 5% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Role of the DPO scope. 77% high assurance, 11% reasonable assurance, 12% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Processor, Third Party Supplier and Controller Relationship Management scope. 93% high assurance, 7% limited assurance.

Governance and Accountability Scope Rating Indicator

Role of the DPO Scope Rating Indicator

Processor, Third Party Supplier and Controller Relationship Management Scope Rating Indicator

The speedometer charts above give a gauge of where the organisation sits on our assurance rating scales from high assurance to very limited assurance.

Areas for Improvement

All processing of personal data by DBS should be documented accurately by completing a comprehensive data mapping exercise. The data mapping should be used to inform the record of processing activity (ROPA) ensuring it is up to date and includes details of all contracts that are in place with data processors.

Complete a training needs analysis (TNA) to ensure that a formally documented role based information governance (IG) and data protection (DP) training programme is provided to staff including the Data Protection Officer (DPO), the Data Protection Team (DP Team), Information Asset Owners (IAOs), other specialist roles, and front line staff collecting and processing personal data.

Staff departmental meetings should include DP/IG agenda items to facilitate ground level issues being discussed and, if necessary, issues escalated to senior management.

Ensure that staff are aware of and have read DP/IG policies and procedures relevant to their role.

Schedule risk based internal audits covering IG and DP and reinstate compliance checks against information management policies and procedures.

Completed data protection impact assessments (DPIAs) should formally record the approval and comments made by the DPO to assist project managers in implementing any DPO recommendations.

DBS privacy policies should be actively communicated to comply with the UK GDPR Right to be Informed.

Best Practice

DBS use a comprehensive contract performance tracker to manage, and risk assess all contracts. This enables them to gain assurance that their data processors and third-party suppliers continue to perform at the correct level and can identify new risks to personal data or organisational security. The tracker includes:

- A risk assessment - high, moderate, or low risk which drives the frequency of "supplier" checks.
- High risk contracts for critical suppliers and/or data processors are checked monthly.
- The assurance framework for high-risk contracts includes the ISO27001 requirements.
- Annual checks are undertaken, and the results recorded on the tracker.
- The dashboard function shows the performance of "suppliers" based on the assessed scores.
- Dates for contracts due to expire and expired.
- The dashboard is used as a reporting tool.

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 DBS.

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