City of London Police

Data protection audit report

August 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.

City of London Police (CoLP) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 22 March 2021 with representatives of CoLP to discuss the scope of the audit.

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

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 with Part 3 of the DPA 2018 are in place and in operation throughout the organisation.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
Role of the Data Protection Officer (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.

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 CoLP 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 June to 8 July 2021. The ICO would like to thank CoLP for its flexibility and commitment to the audit during difficult and challenging circumstances.

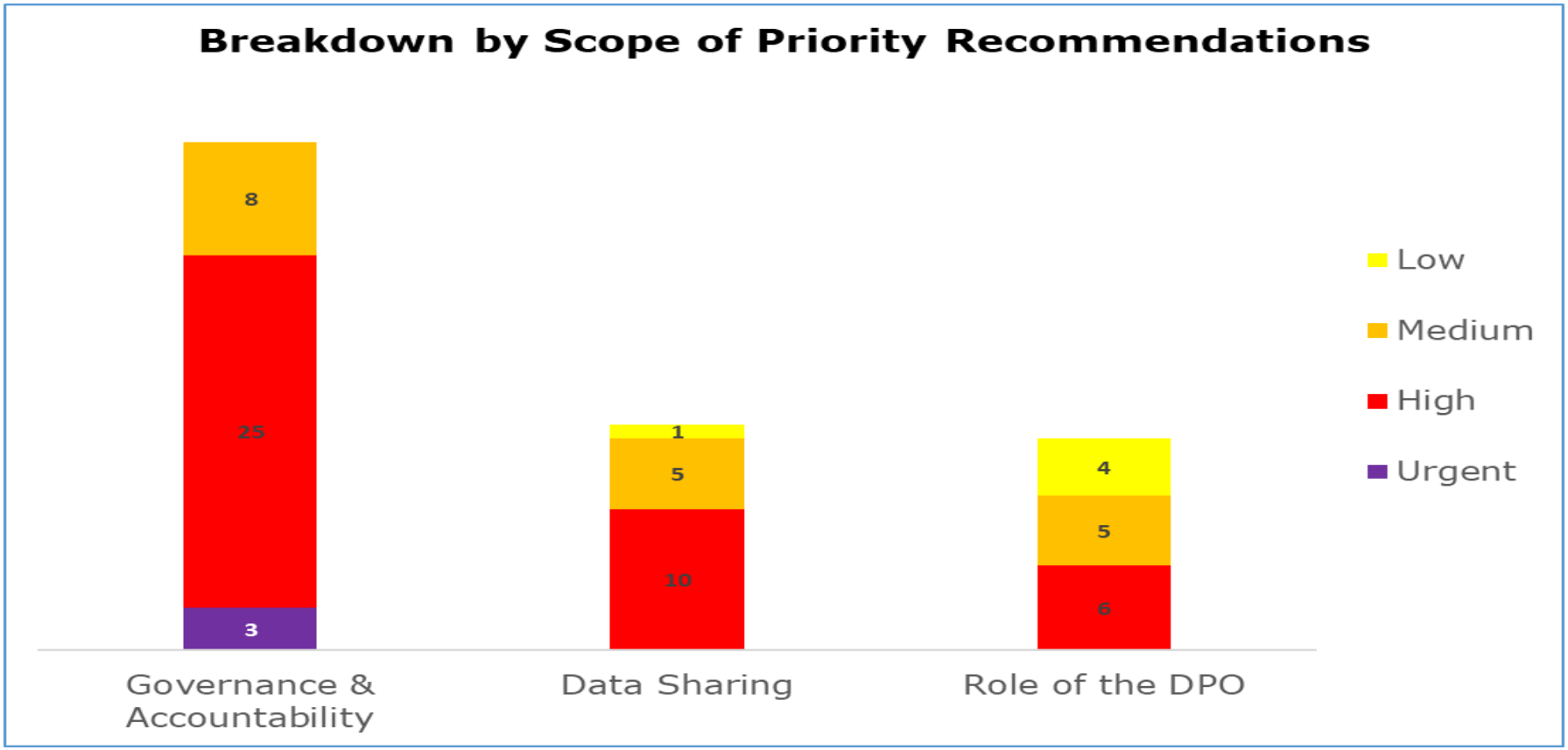
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist CoLP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. CoLP'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	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Role of the DPO	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.

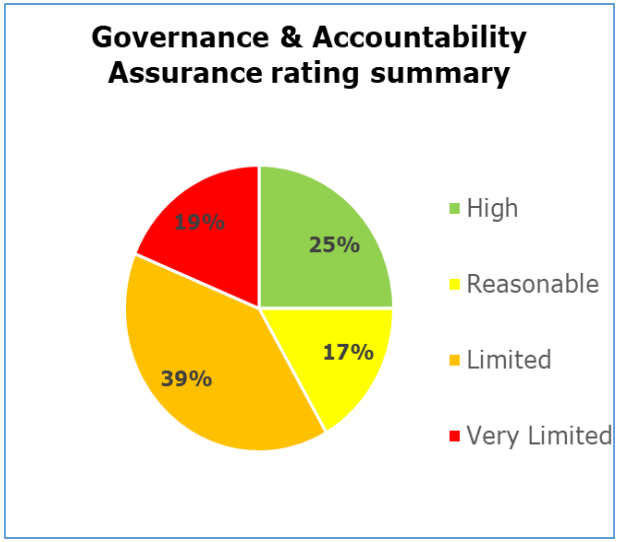
Priority Recommendations

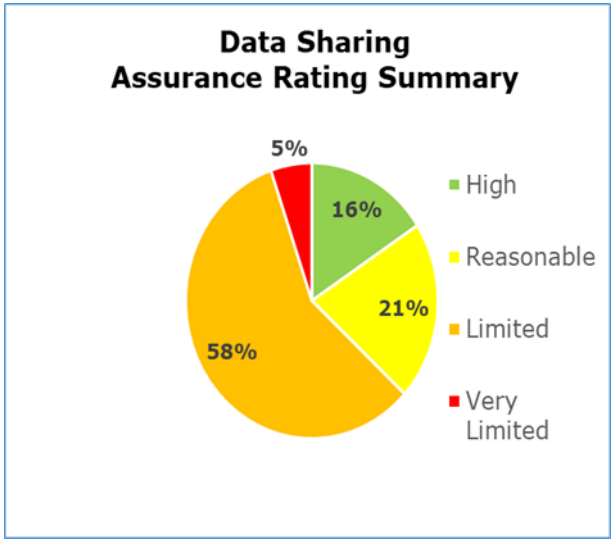


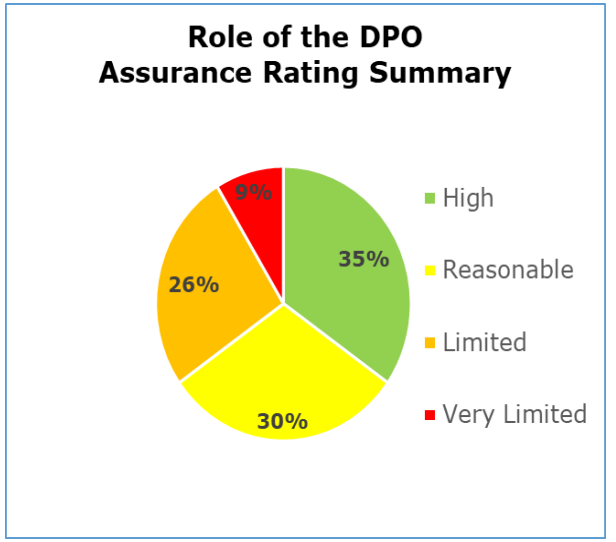
The bar chart shows a breakdown by scope area of the priorities assigned to our recommendations made.

- Governance and accountability scope has 3 urgent, 25 high and 8 medium priority recommendations
- Data sharing scope has 10 high, 5 medium and 1 low priority recommendations
- Role of the DPO scope has 6 high, 5 medium and 4 low priority recommendations

Graphs and Charts







The pie charts show a summary of the assurance ratings awarded in the governance and accountability (G&A) scope, the data sharing (DS) scope and the role of the DPO scope. For the G&A scope 25% high assurance, 17% reasonable assurance, 39% limited assurance and 19% very limited assurance. For the DS scope 16% high assurance, 21% reasonable assurance, 58% limited assurance and 5% very limited assurance. For the role of the DPO scope 35% high assurance, 30% reasonable assurance, 26% limited assurance and 9% very limited assurance.

Areas for Improvement

The completion of a Learning Needs Analysis (LNA) will inform the information governance (IG) and data protection (DP) training programme. Specialist training for DP roles including the DPO, and information asset owners (IAOs) is required beyond the basic training provided to all staff. Specialist training is required within functions: records management (RM) teams, subject access request (SARs) teams, information security (IS) and staff making data sharing decisions, including the specific law enforcement provisions of Part 3 of the DPA18.

Under resourcing and staff vacancies within the Information Management Directorate have resulted in backlogs relating to the management of information sharing agreements, deletion of records and completion of Data protection impact assessments (DPIAs) all of which present a serious risk of non-compliance with DP legislation.

A programme of risk-based IG audits should be initiated as part of an internal audit plan. Risk identification and management can be augmented by a regular programme of independent external audits. The programme of audits can support monitoring of staff compliance with DP policies and procedures.

A comprehensive, detailed data mapping exercise is required for all information assets and processing activities, to create an overarching record of processing activities (ROPA) which is reviewed on a regular basis. The exercise is key to comply with section 61 of the DPA18 legislation and establishing the lawful basis for processing personal data and sensitive processing.

Ensuring that there are key performance indicators (KPIs) in place that are reported and reviewed regularly at Board meetings. KPIs for SARs, IG/DP training completion, RM, security breaches and near misses will help provide oversight and understanding of the effectiveness of control measures.

Established sharing of personal data requires a review to ensure there are appropriate data sharing agreements in place and to confirm the data sharing aligns with the statutory requirements of the ICO Data Sharing Code of

practice. Existing sharing agreements should be reviewed to establish the effectiveness of partners security measures and their retention and deletion processes.

Using consent as a lawful basis for general processing (Part 2) and law enforcement (Part 3) processing should be revisited to ensure it meets the provisions of the DPA18. It must be specific, require a positive opt-in and easy for data subjects to withdraw their consent.

Logging of automated law enforcement processing systems (any IT database) needs to be completed for all CoLP systems to meet section 62 of the DPA 2018 requirements. The effectiveness of any processors logging systems should also be routinely checked.

Best Practice

CoLP have added the DPIA template as an appendix to the information sharing agreement (ISA) template. This will ensure that DPIA screening and, or completion is undertaken for all proposed new data sharing arrangements to identify the risks, benefits and appropriate controls

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 CoLP.

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