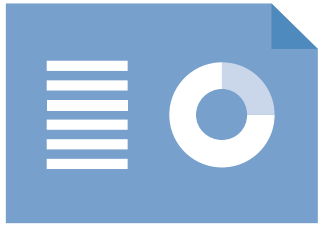
Liverpool City Council

Data protection audit report

July 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.

Liverpool City Council (LCC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 27 May 2020 with representatives of LCC to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and LCC with an independent assurance of the extent to which LCC, 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 & 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.
Information Security (Security of Personal Data)	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Freedom of Information (FOI)	The extent to which FOI accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

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, LCC 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 July 2020 to 30 July 2020. The ICO would like to thank LCC for its flexibility and commitment to the audit during difficult and challenging circumstances.

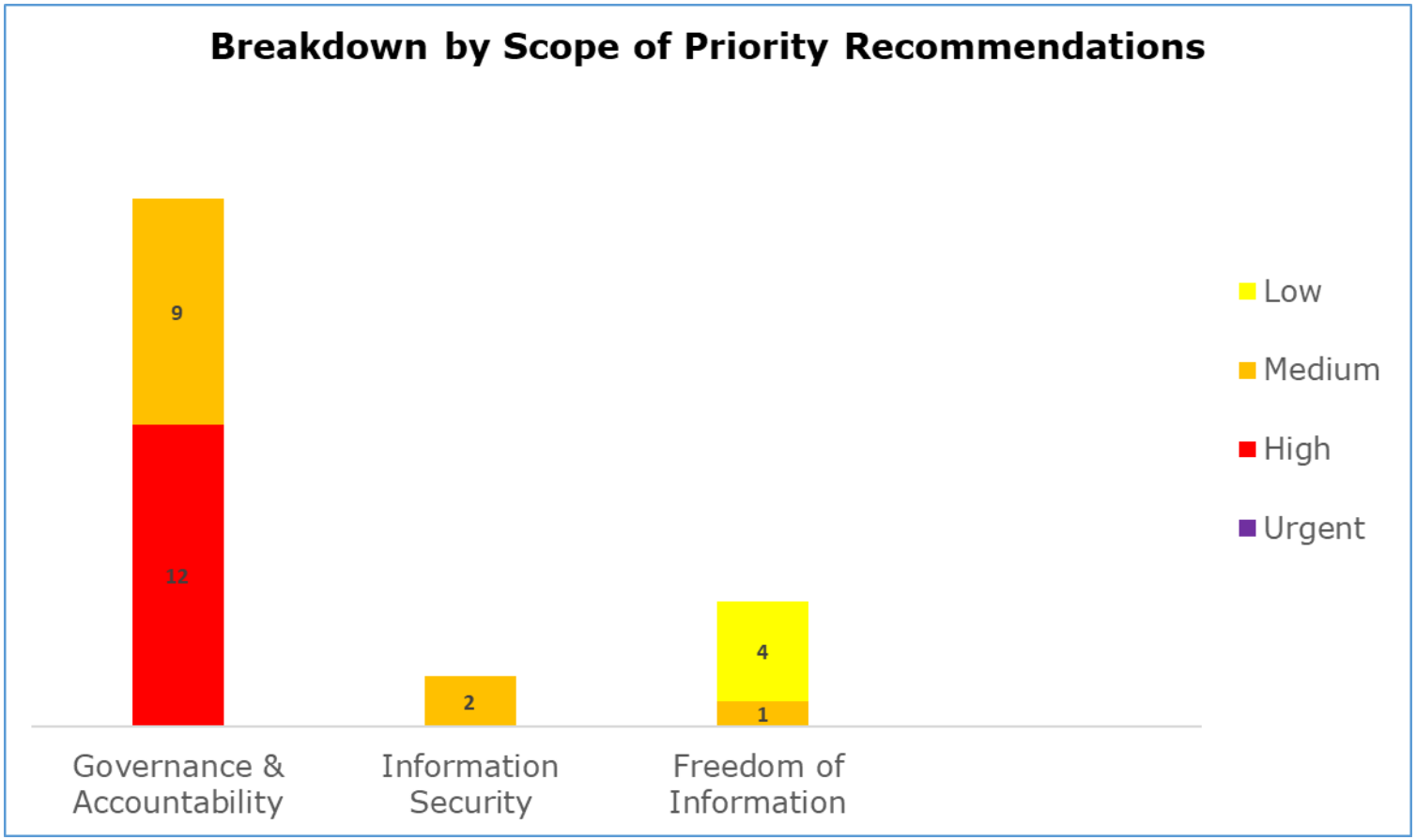
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist LCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. LCC'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 & 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.
Information Security	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.
Freedom of Information	High	There is a high level of assurance that processes and procedures are in place and are delivering compliance with Freedom of Information legislation . 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



Areas for Improvement

Job descriptions for information governance roles should be created formally documenting the responsibilities of each role.

20.08.20

Action should be taken to ensure the Record of Processing Activities accurately reflects all the personal information the Council processes and provides sufficient detail of this processing.

The requirement for a lawful basis to be established for the new processing of personal data, along with the creation of a Data Protection Impact Assessment (DPIA) where appropriate, should be included in a formalised process.

Individuals should receive privacy information at the point they provide personal data to the Council via online and paper format forms.

Ensure training materials are updated to include the fact that EIR Requests can be made both verbally and in writing.

Ensure that the responsibilities of the Deputy Head of Democratic Services & Information Manager and the City Solicitor and SIRO are documented within the IG Framework.

Create a standard checklist or form which can be used to record findings showing both adherence to procedures and good practice in use of exemptions, redactions and areas for improvement.

Best Practice

LCC's training modules can be easily accessed by all staff in an interactive format or in a word/pdf format for staff who do not have computer access or who require a screen reader for sight loss. Further to this LCC provide face to face training sessions and workshops for staff where appropriate. LCC has taken great care to ensure that its training is available in an accessible format for all staff.

LCC require their device suppliers to asset tag any new devices with a list of available asset numbers supplied by LCC. This ensures that once the devices are received by LCC they can be enrolled within the Configuration Management Database and help maintain an up to date asset inventory.

Files are protected with a security application that monitors for unauthorised access to confidential files and provides an audit trail of confidential file movements across the LCC network.

Authorised staff are provided with a viewing area within the physical records secure area to help prevent the unauthorised removal or accidental loss of confidential data. A member of the records management team is always present when authorised personnel are in the physical records secure area.

Access lists are maintained as to who has authorisation to access LCC server rooms and who can authorise access to the server rooms.

Business Continuity plans include provisions for remote workers to still access information and keep information secure.

There is an FOI & EIR Champions Group in place which meets quarterly to discuss performance rates, key issues, best practice, updates to guidance and development training.

LCC proactively publish official recorded information on its website for everyone to access.

Where a third party processor is being used there are clear clauses within the contract for handling FOI/EIR requests for example, transferring the request to the controller, the controller's discretion for releasing information and assisting the controller in responding to a request.

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 Liverpool City Council.

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