Hertfordshire County Council

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.

Hertfordshire County Council (HCC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 19 May 2021 with representatives of HCC to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and HCC with an independent assurance of the extent to which HCC, 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 HCC processing of personal data. The scope may take into account any data protection issues or risks which are specific to HCC, identified from ICO intelligence or HCC'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 HCC, the nature and extent of HCC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to HCC. 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 UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
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.
Freedom of Information	The extent to which FOI/EIR 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 HCC 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 10 August to 12 August 2021. The ICO would like to thank HCC for its flexibility and commitment to the audit during difficult and challenging circumstances.

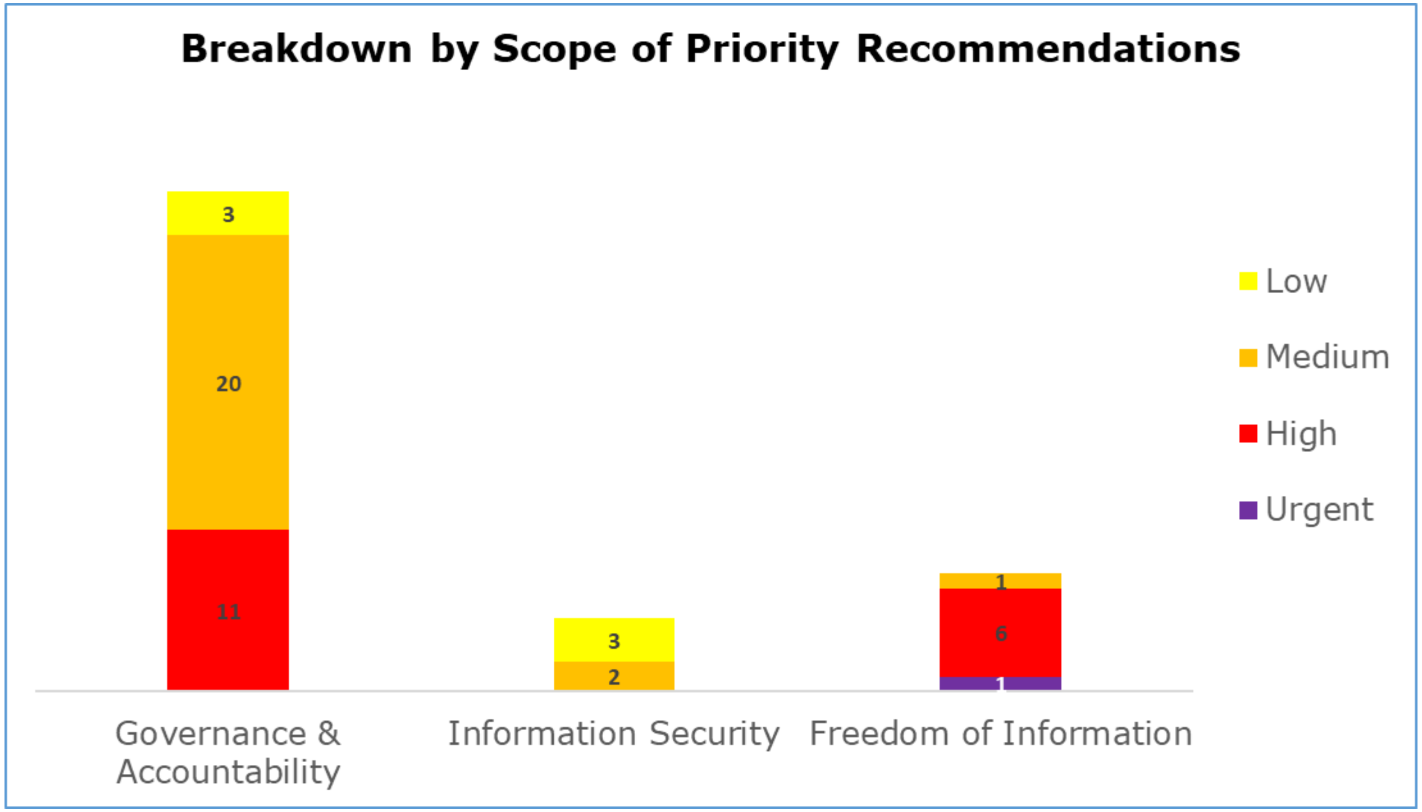
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection and freedom of information legislation. In order to assist HCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. HCC'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	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified considerable 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 above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 11 high, 20 medium and three low priority recommendations
- Information Security, two medium and three low priority recommendations
- Freedom of Information has one urgent, six high and one medium priority recommendations

Areas for Improvement

There is a formal information governance (IG) group in place but it doesn’t include membership from across the organisation. HCC should create an expanded IG group with responsibility for oversight of compliance with IG matters. IT should also sit in this group to ensure that there is joined up and documented governance links between the IG and IT functions.

IG policies currently lack a compliance section. A compliance section should be documented within all key IG policies setting out how compliance with those policies will be monitored at both local service and corporate levels.

HCC should formalise a schedule of periodic recorded security checks for clear desks and screens for when staff return to the office.

Periodic documented risk assessments for all secure areas across the HCC estate should be instigated to mitigate any unrecognised risks that could lead to unauthorised access to personal or special category data.

HCC does not currently have a documented FOI policy. HCC should implement an FOI policy to formally document its processes and procedures, thus ensuring it is able to demonstrate its compliance with the relevant legislation.

A quality assurance process for FOI responses should be established. Peer reviews, dip-sampling, and cold case reviews should be undertaken, with results recorded and fed back to the proposed Information Governance Group as well as the staff involved in the original request.

HCC’s FOI training does not record the results of the concluding quiz, and as such there is no way of measuring learner knowledge on completion of the module. HCC should document the results of this quiz, to monitor both staff knowledge and the efficacy of the learning materials.

Best Practice

The IG function is supported by experienced subject matter experts with suitable qualifications.

HCC have a Metacompliance tool in place to monitor compliance around policies.

HCC is very focused on improving cyber security awareness amongst its staff and is using a number of innovative methods and communication channels in order to achieve this. Systems record the effectiveness of these methods, and alongside user feedback has given HCC the ability to adapt and refine the various campaigns to create targeted learning outcomes. This will ensure that staff can fully play their part in enabling HCC to maintain high levels of information security.

The use of daily penetration testing, both internal and external, on HCC's information infrastructure coupled with a planned test period during the application of software patches; should minimise the risk of a software vulnerability being exploited in a cyber-attack.

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