Health and Safety Executive

Data protection and freedom of information audit report

October 2024

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation, UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), as well as the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

Section 129 of the DPA 2018 allows the ICO to carry out consensual audits. Section 47 of the FOIA provides provision for the Commissioner to assess whether a public authority is following good practice, including compliance with the requirements of this Act and the provisions of the codes of practice under sections 45 and 46.

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 Health and Safety Executive (HSE) agreed to a consensual audit of its data protection, FOIA and EIR requirements. The purpose of the audit is to provide the Information Commissioner and HSE with an independent assurance of the extent to which HSE, within the scope of this agreed audit, is complying with data protection legislation, FOIA and EIR requirements.

The scope areas covered by this audit are determined following a risk based analysis of HSE's processing of personal data. The scope may take into account any data protection, FOIA or EIR issues or risks which are specific to HSE, identified from ICO intelligence or HSE'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 HSE, the nature and extent of HSE's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to HSE.

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 UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Training and Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.
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 public authority.

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.

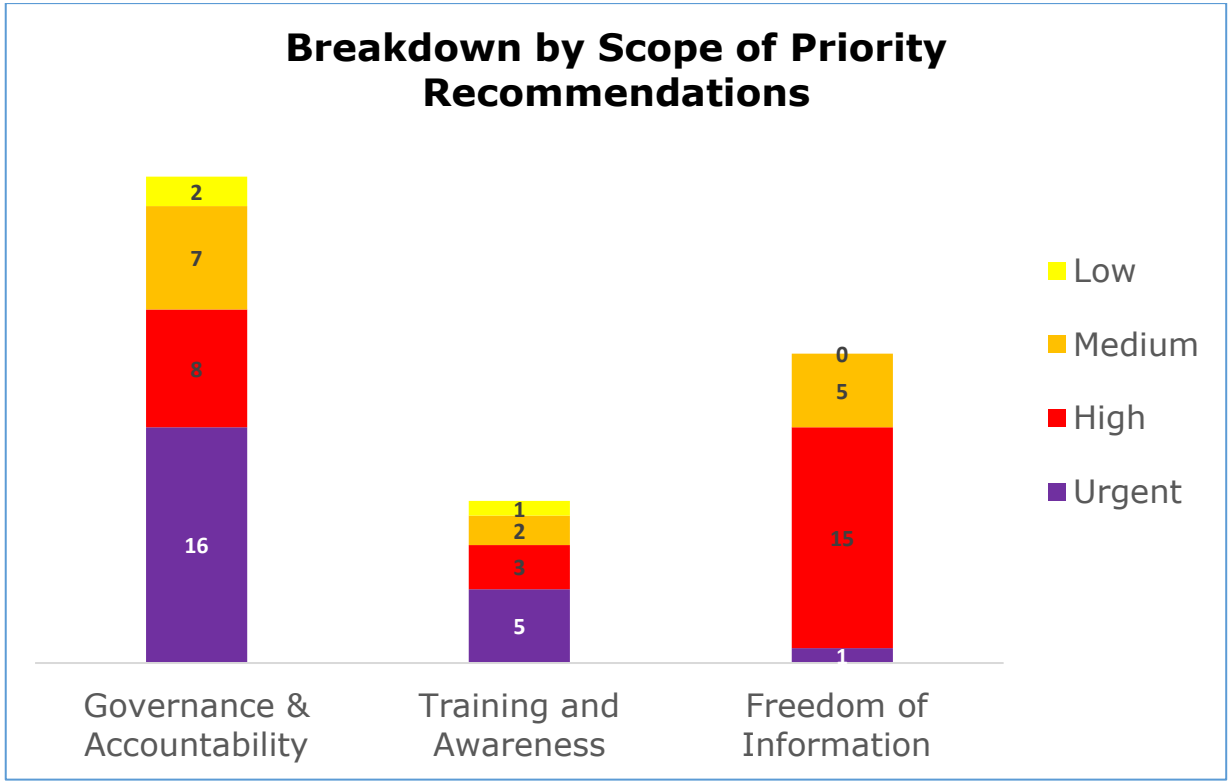
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist HSE in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. HSE'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.
Training and Awareness	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.
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 freedom of information legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

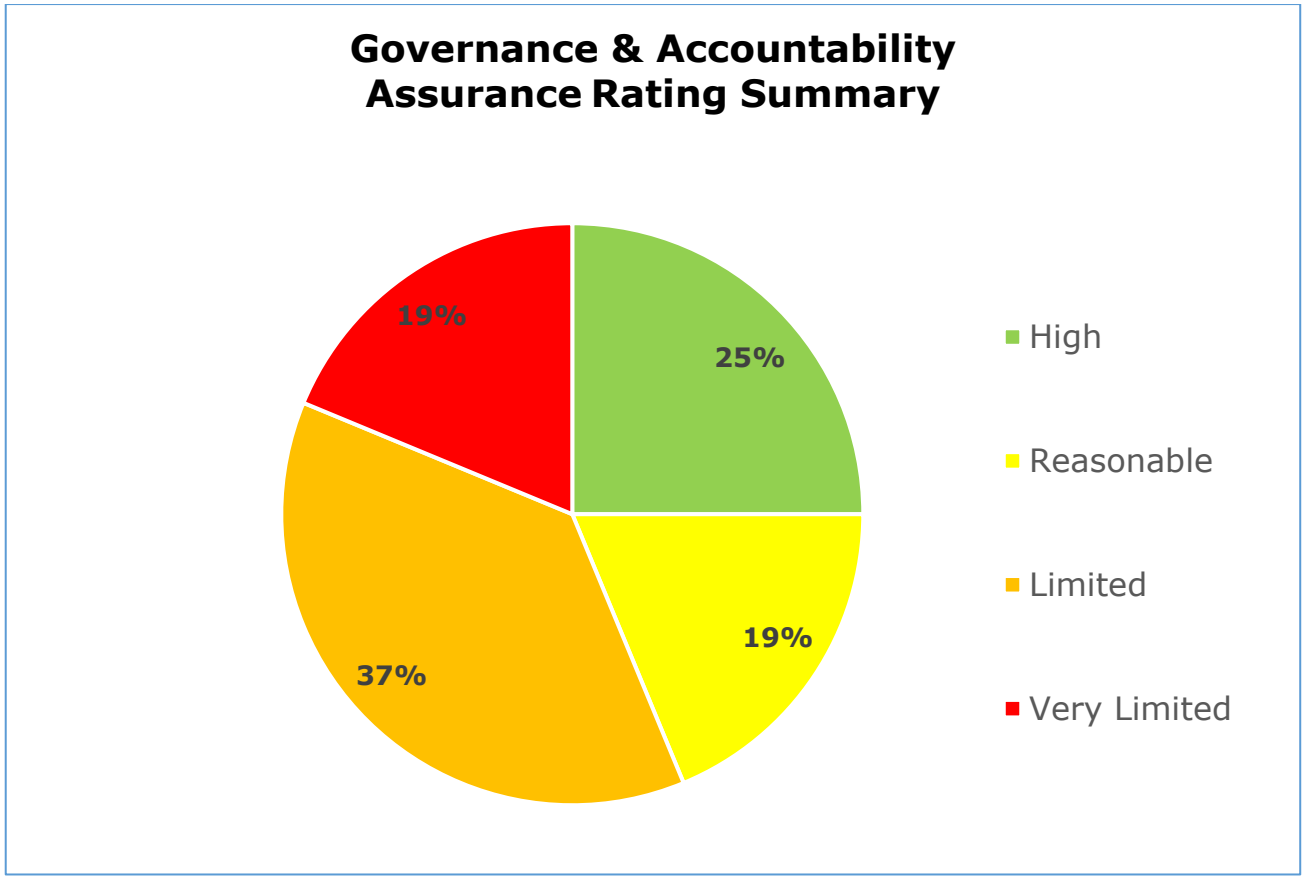
Priority Recommendations



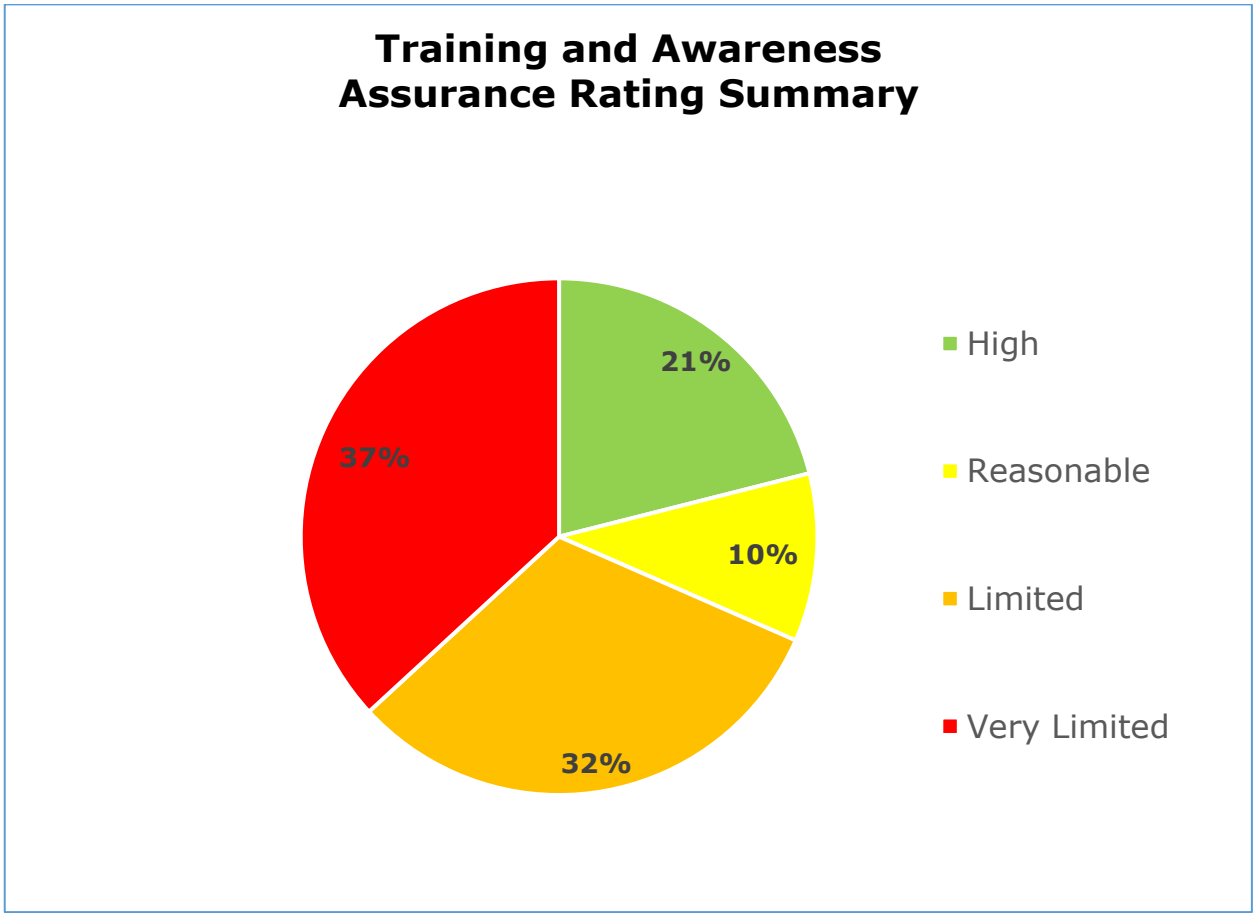
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 16 urgent, eight high, seven medium and two low priority recommendations
- Training and Awareness has five urgent, three high, two medium and one low priority recommendations
- Freedom of Information has one urgent, 15 high, five medium and no low priority recommendations

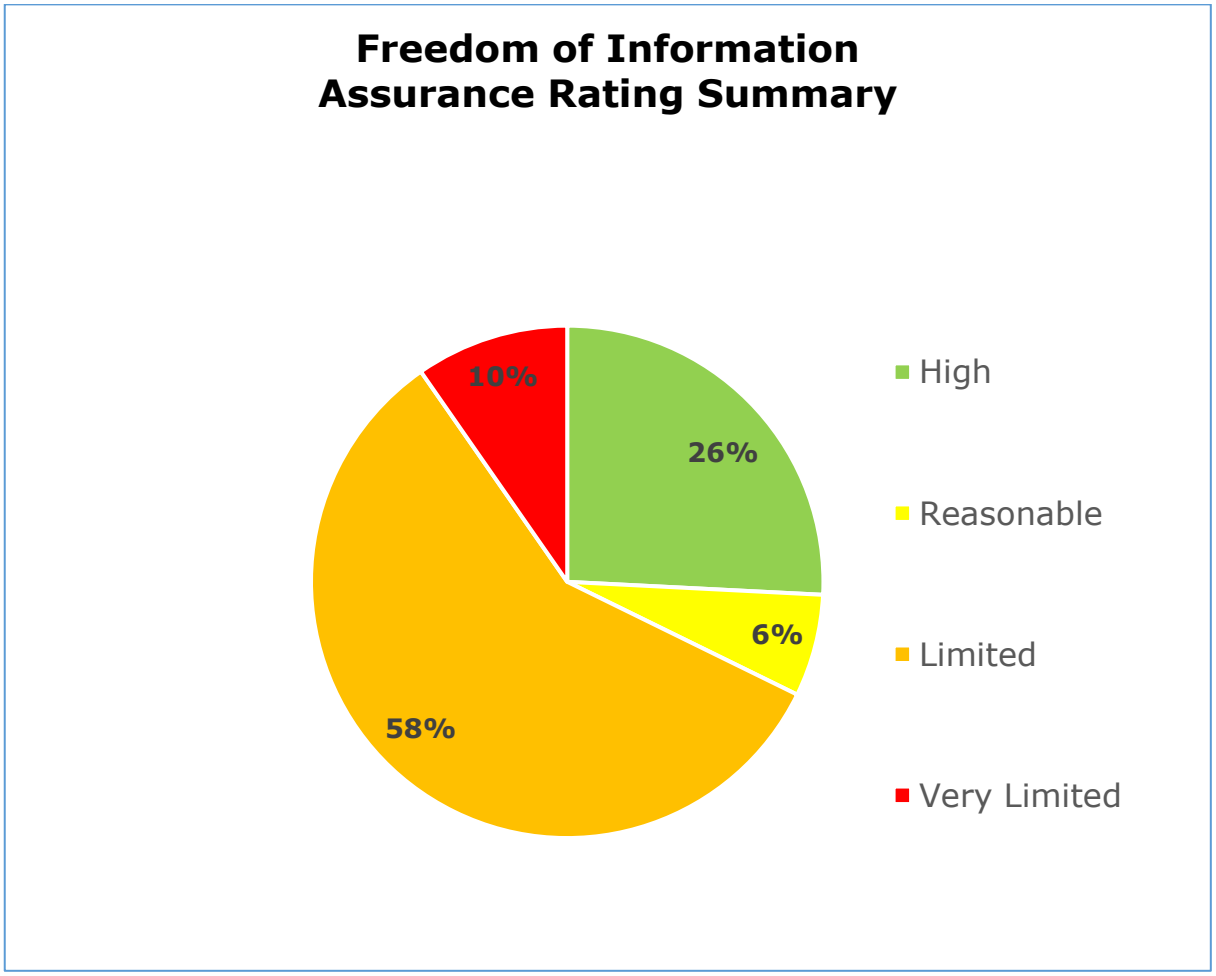
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 25% high assurance, 19% reasonable assurance, 37% limited assurance, 19% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Training and Awareness scope. 21% high assurance, 10% reasonable assurance, 32% limited assurance, 37% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Freedom of Information scope. 26% high assurance, 6% reasonable assurance, 58% limited assurance, 10% very limited assurance.

Key areas for improvement

We identified some key areas within our audit where HSE needed to implement further measures to comply with data protection law.

Governance and Accountability

- HSE must ensure that their organisational structure allows for the Data Protection Officer (DPO) to have oversight and accountability for all areas of UK GDPR and DPA 2018 compliance.
- HSE must ensure the ROPAs are clear, accurate and contain all the required information.
- HSE should ensure that they have assurances of data protection compliance through compliance checks, internal audits and external audits, and that risks found during these activities are properly recorded, managed and/or mitigated as appropriate.

Training and Awareness

- HSE should ensure that IG training material is sufficiently comprehensive, accurate and relevant to the data processing HSE undertakes.
- HSE should ensure all staff receive the necessary IG training that is effective and specific to their role, within an appropriate timeframe.
- HSE should establish KPIs and reliable reporting mechanisms to monitor staff completion of the mandatory IG training.

Freedom of Information

- HSE should ensure that their information management processes are followed in order for information to be stored correctly and made readily available when FOI/EIR requests are received.

- HSE should finalise their FOI/EIR policies and procedures in order for all staff to have an understanding of how HSE handles FOI/EIR requests from receipt to provision of a response.
- HSE should continue to improve their internal review compliance to ensure that responses to complaints are provided in a timely manner.

Key areas of assurance

At the time of the audit and based on the evidence seen by auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

Governance and Accountability

- HSE have a DPO in place who demonstrated a good level of knowledge and has started putting measures into place to address risks which they identified prior to the audit.

Training and Awareness

- Staff demonstrated an understanding of the shortcomings of the current training programme and some work is already underway, or is planned, to help resolve some of the issues around HSE's training and awareness provisions.

Freedom of Information

- HSE have various FOI templates in place to support staff with responding to FOI requests.
- HSE conduct monthly quality assurance dip sampling checks on completed FOI/EIR responses to provide a high level overview of performance.

Best Practice

Training and Awareness

- HSE has sought feedback on the Information Security corporate induction training material from an external sector specialist to gain objective and expert advice.

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 Health and Safety Executive.

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