Tameside Metropolitan Borough Council

Data protection and freedom of information audit report

September 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.

Tameside Metropolitan Borough Council (TMBC) agreed to a consensual audit of its data protection practices. The purpose of the audit is to provide the Information Commissioner and TMBC with an independent assurance of the extent to which TMBC, 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 TMBC's processing of personal data. The scope may take into account any data protection, FOIA or EIR issues or risks which are specific to TMBC, identified from ICO intelligence or TMBC's own concerns, as well as any 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 TMBC, the nature and extent of TMBC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to TMBC.

It was agreed that the audit would focus on the following areas:

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 TMBC.
The role of the Data Protection officer (DPO)	The extent to which TMBC has complied with their obligations under UK GDPR to appoint an independent DPO who is properly trained and resourced.
Personal data breach management and reporting	The extent to which the TMBC has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate.
Requests for access and data portability	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.
Freedom of Information (FOI)	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 TMBC.

Audits are conducted following the Information Commissioner's audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both onsite and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential documentation.

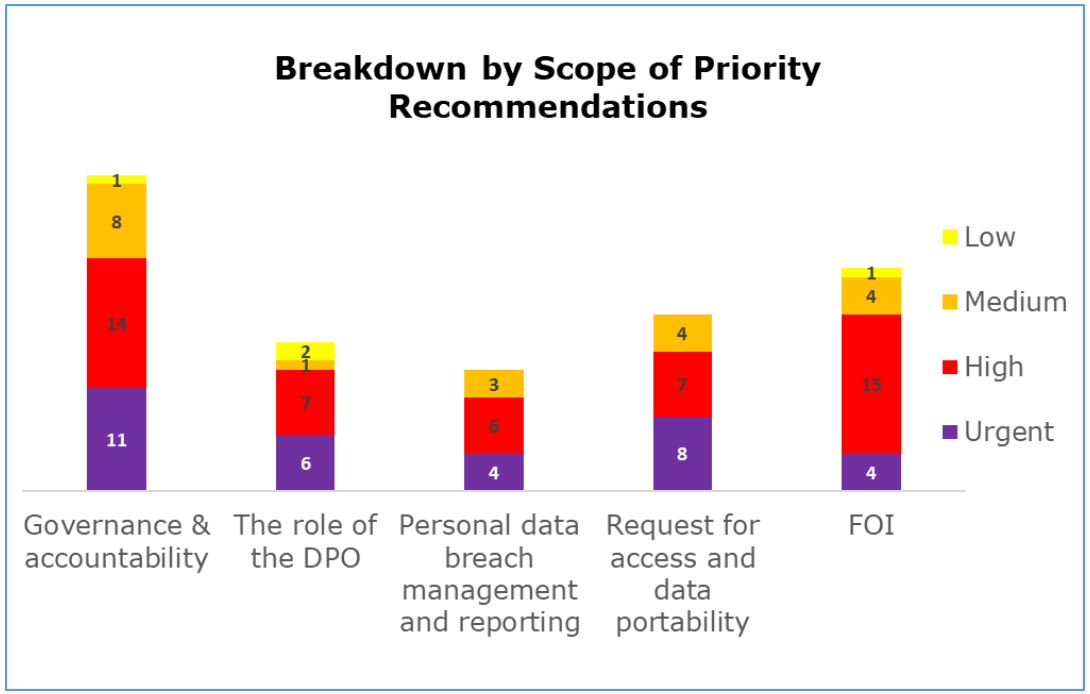
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection and FOI legislation. In order to assist TMBC in implementing the recommendations each has been assigned a priority rating based upon the risks that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

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

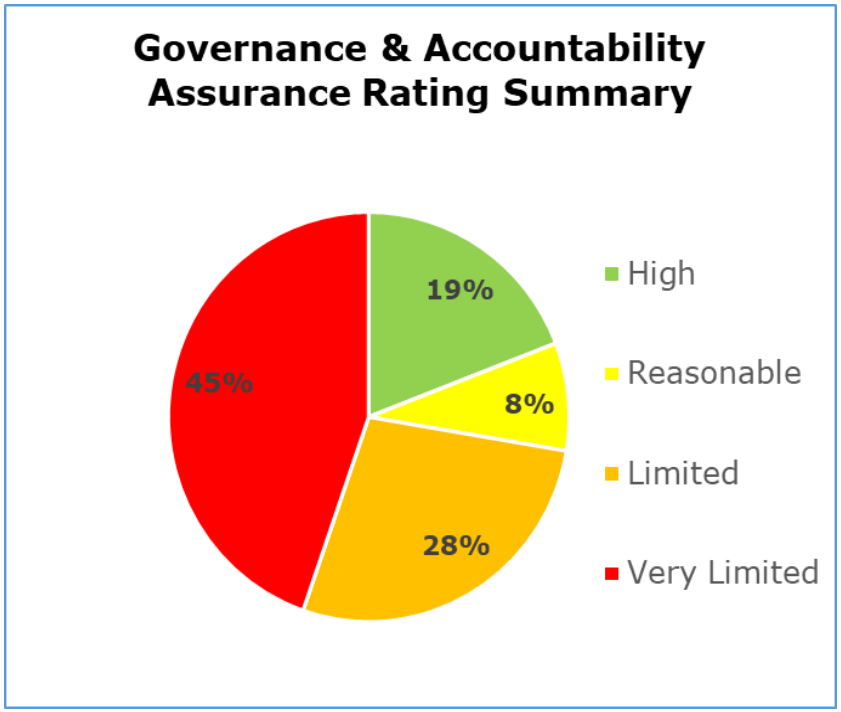
Priority Recommendations



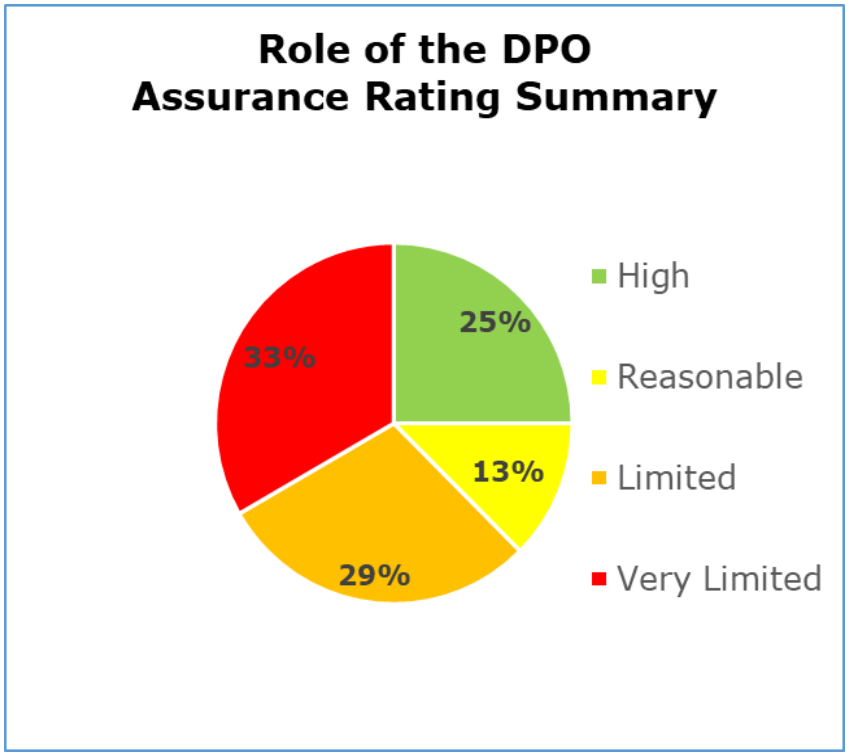
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and accountability has 11 urgent, 14 high, eight medium and one low priority recommendations
- The role of the DPO has six urgent, seven high, one medium and two low priority recommendations
- Personal data breach management and reporting has four urgent, six high, three medium and no low priority recommendations
- Request for access and data portability has eight urgent, seven high, four medium and no low priority recommendations
- FOI has four urgent, 15 high, four medium and one low priority recommendations

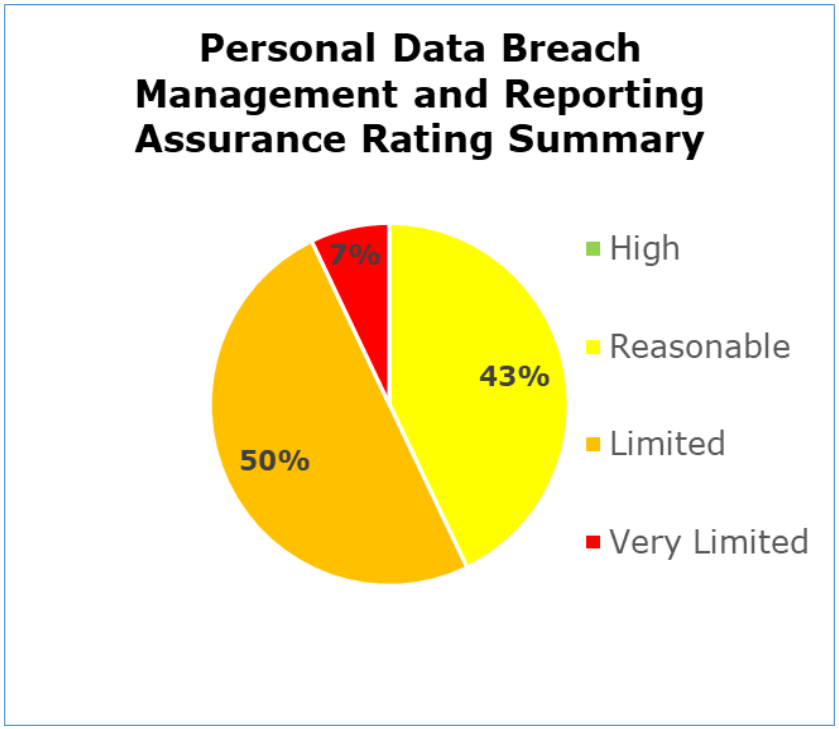
Graphs and Charts



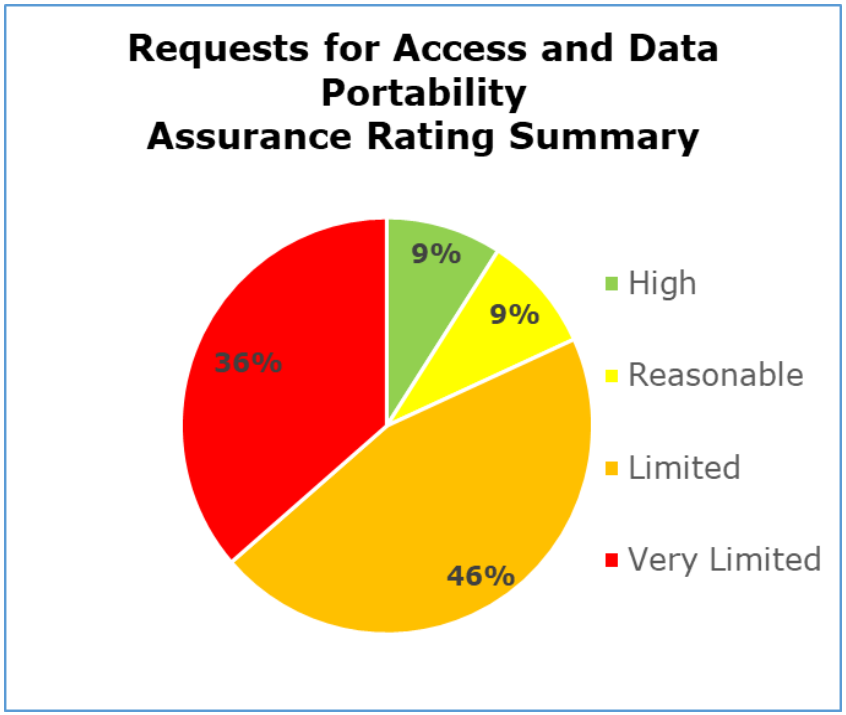
The pie chart above shows a summary of the assurance ratings awarded in the governance and accountability scope. 19% high assurance, 8% reasonable assurance, 28% limited assurance, 45% very limited assurance.



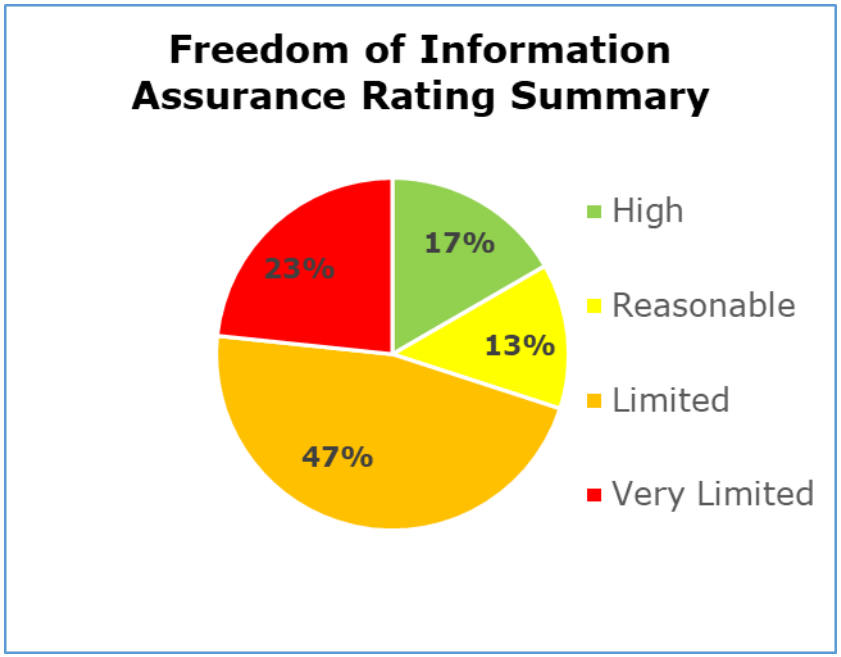
The pie chart above shows a summary of the assurance ratings awarded in the role of the DPO scope. 25% high assurance, 13% reasonable assurance, 29% limited assurance, 33% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the personal data breach management and reporting scope. 0% high assurance, 43% reasonable assurance, 50% limited assurance, 7% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the requests for access and data portability scope. 9% high assurance, 9% reasonable assurance, 46% limited assurance, 36% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the FOI scope. 17% high assurance, 13% reasonable assurance, 47% limited assurance, 23% very limited assurance.

Areas for Improvement

Governance and accountability

- TMBC has a largely new senior management information governance (IG) team who are focused on identifying IG development areas and reviewing existing IG practices, to improve the Council's performance and to meet regulatory requirements. The current IG structure and framework does not support TMBC in meeting governance and accountability regulatory requirements for which the Council has also recognised and plans are being formulated to address. In addition, not all staff with IG and data protection (DP) responsibilities have a clear understanding of their roles and responsibilities nor have they been clearly documented, for example, in job descriptions.
- TMBC have recently reviewed and updated its DP policies, but additional areas of improvement have been highlighted as part of the ICO audit. TMBC are in the process of reviewing its DP procedures and this work must be completed.
- The current mandatory IG and DP training does not provide the necessary detail, and there is no requirement for staff to read IG and DP policies and procedures. Staff with specific DP responsibilities have not completed appropriate training and no training needs analysis (TNA) has been conducted to establish the training needs of specific roles in respect of IG responsibilities.
- Formal, regular, quality assurance (QA) checks are not in place across all areas of the Council. TMBC should document how it will monitor adherence to its DP related policies and procedures and ensure compliance to these requirements through formal and routine QA monitoring.
- TMBC must complete the information audit and the review of its record of processing activities (ROPA) that it has begun. TMBC must ensure the ROPA contains relevant, accurate and up to date information. The Council must then ensure it is regularly reviewed so it remains fit for purpose. The ROPA should be used to improve

IG and help TMBC comply with DP legislation, for example, keeping personal data secure, records management and creating privacy notices.

- Privacy notices do not contain all relevant information as required by Articles 13 and 14 of the UK GDPR. Furthermore, data subjects are not reliably made aware of privacy information when their data is collected, or in instances where their personal data has been obtained from a source other than themselves.

The role of the DPO

- Whilst TMBC have appointed a DPO it has not recorded this decision fully, including any conflict of interest considerations, which would help the Council demonstrate compliance with the accountability principle and DP legislation. Furthermore, the DPO's role and responsibilities have not been fully documented.
- The DPO is undertaking specialist DPO training, however they are yet to complete this training. Without expert knowledge of DP, the DPO may not be able to fulfil tasks related to UK GDPR Article 39.
- TMBC is lacking an organisation structure which provides the DPO with strong oversight for managing DP and IG, and it does not have a documented process for the escalation of DP matters. Without the defined and documented processes, work could be carried out without DPO oversight or advice, which could result in a breach of DP legislation.

Personal data breach management and reporting

- There is a strong focus on technical measures to prevent and detect personal data breaches (PDBs), however organisational and physical measures require improvements as ICO auditors identified risks in these areas that if not mitigated could result in a PDB.
- TMBC do not have documented contingencies for breaches that occur out of hours or in the case of decision maker absence. This risk delays to reporting to the ICO when required.

- The training provided to staff does not sufficiently cover PDBs and the internal procedure to report them. This risks breaches not being identified or being reported to the ICO when required.

Requests for access and data portability

- TMBC is currently not meeting statutory timeframes for responding to requests. Though there have been discussions around ways to streamline the process, there is currently a lack of resource in certain service areas that has not yet been addressed.
- Data mapping exercises are ongoing, therefore TMBC does not have full awareness of the information it holds and where it is held. As such, processes for locating and retrieving information required for a request are sometimes hindered, and retention schedules for both responses to requests as well as organisation-wide data are not always adhered to.
- Not all staff involved in the process of handling subject access requests (SARs) have received role-specific training to ensure full awareness of their responsibilities and the application of the legislation. This includes the use of exemptions and redactions, and staff responsible for QA processes.

FOI

- TMBC is currently not meeting statutory timeframes for responding to requests. Though there have been discussions around ways to streamline the process, there is currently a lack of resource that has not yet been addressed.
- As above, data mapping exercises are ongoing, and as such TMBC does not have full awareness of the information it holds and where it is held. As a result, processes for locating and retrieving information required for a request are sometimes hindered.
- As with SARs, not all staff involved in the handling of FOI/EIR requests have received role-specific training. TMBC has yet to complete a TNA to identify appropriate training for all staff involved in the process.

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