Greater Manchester Police

Data protection audit report

January 2022

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 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.

Greater Manchester Police (GMP) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 3 September 2021 with representatives of GMP to discuss the scope of the audit.

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

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 DPA18 and other 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.
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.

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, GMP 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 8 November to 19 November 2021. The ICO would like to thank GMP for its flexibility and commitment to the audit during difficult and challenging circumstances.

A pre-audit survey was launched to all GMP staff, and we received 916 responses, which represents approximately 10% of GMP employees. ICO Auditors were pleased to note that the survey was completed by a range of operational and non-operational staff from across departments in GMP. The respondents had a range of time-served within GMP with the majority having worked for GMP for over 10 years.

The survey consisted of 32 optional questions which were based on information security and data protection training and awareness, in line with the agreed scope areas.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist GMP 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. GMP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

In addition to this consensual ICO data protection audit, GMP agreed to the ICO reviewing updates on their progress with implementing the recommendations and actions to mitigate the risks from the HMICFRS VSA report published in December 2020.

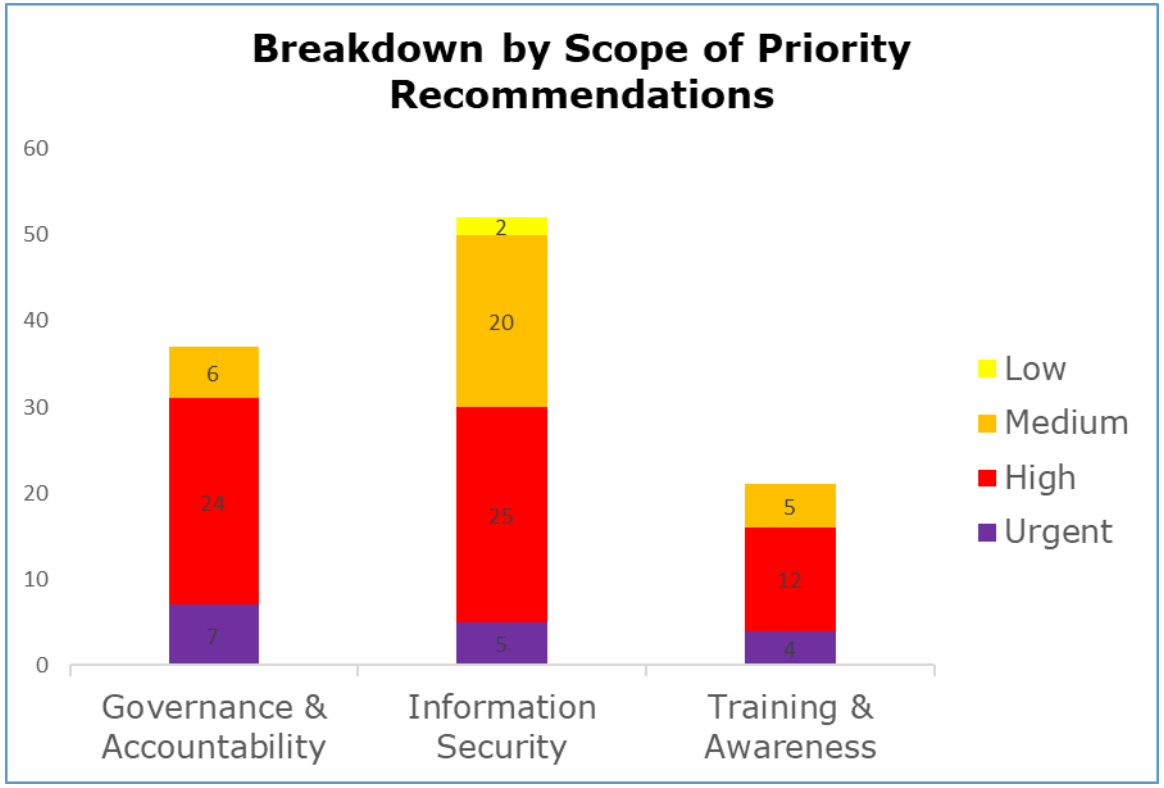
The aim of this review is to provide the Information Commissioner with assurance that GMP have identified, and are appropriately addressing, all the data protection risks arising from the HMICFRS VSA report findings and any that may not have been previously considered, to ensure compliance with data protection legislation

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.
Information Security	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.

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.

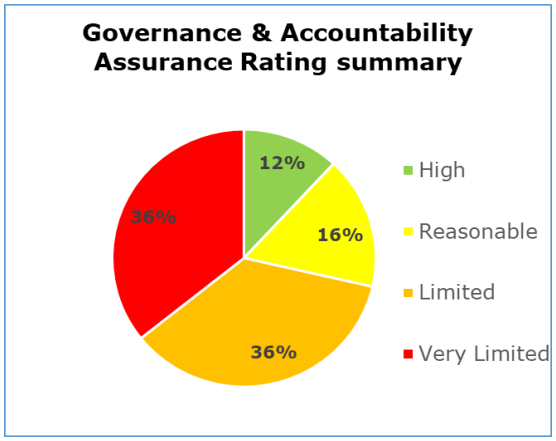
Priority Recommendations



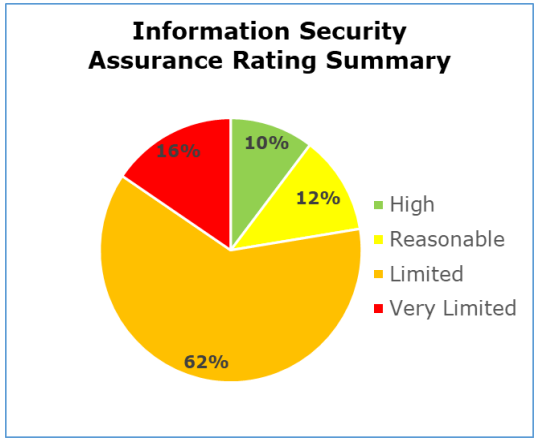
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 7 urgent, 24 high and 6 medium priority recommendations
- Information Security has 5 urgent, 25 high, 20 medium and 2 low priority recommendations
- Training and Awareness has 4 urgent, 12 high and 5 medium priority recommendations

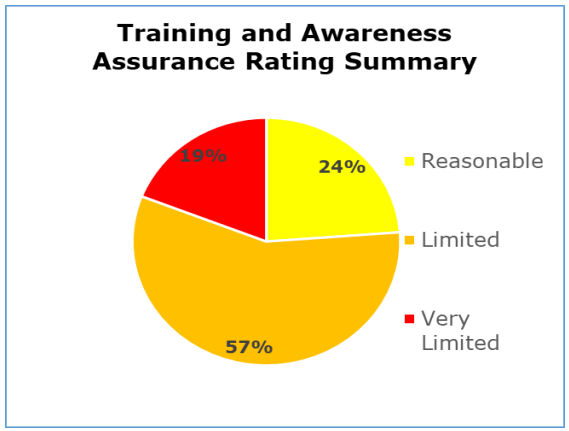
Graphs and Charts



The pie charts above show a summary of the assurance ratings awarded in the governance and accountability scope. 12% high assurance, 16% reasonable assurance, 36% limited assurance, 36% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the information security scope. 10% high assurance, 12% reasonable assurance, 62% limited assurance, 16% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the training and awareness scope. 24% reasonable assurance, 57% limited assurance, 19% very limited assurance.

Areas for Improvement

- Ensure that GMP have sufficient dedicated resource from their data protection officer (DPO) and that there are appropriately resourced operational roles in place, to support the day to day management of all aspects of IG and data protection. The vacant positions in Information Compliance are impacting on the resourcing levels of information security (IS) and records management (RM) staff and presents a serious risk of non-compliance with data protection (DP) legislation.

- Complete the Appropriate Policy Document (APD) to include GMP's procedures for complying with the DP principles in its processing of personal data under Part 3 of the DPA18.

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

- Further work is required to complete the risk assessments on all departmental information assets, and to update them on at least a quarterly basis, and formally document them in an up to date risk register. This will help senior management to understand the business impact of all personal data related risks and manage them effectively.

- Information management policies and procedures require updating and finalising so that they are in line with UKGDPR, Part 2 and Part 3 of the DPA18. The procedures for reporting security incidents, appropriate use of information and technology and the access controls to IT systems need to be formalised and followed Force wide.

- The Information Assurance Board (IAB) needs to convene more frequently and agree an action plan to manage issues and risks with information governance (IG) and DP compliance. The IAB approving policies and procedures, together with regular review will provide oversight and provide assurance of their effectiveness.

- Ensure that there are key performance indicators (KPIs) in place across all IG processes and that they are reported and reviewed regularly at IAB meetings. KPIs for subject access requests (SARs), IG/DP training completion, RM, IS breaches and near misses will help provide oversight and understanding of the effectiveness of control measures.

- Routinely monitor the logging conducted on all IT databases used for law enforcement processing for inappropriate access, or disclosure of personal data and to ensure the integrity and security of personal data.

- 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.

- Using consent as a lawful basis for general processing (Part 2) and/or 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.

- Complete a training needs analysis (TNA). Regularly assess the IG training needs of all staff and ensure the training programme is supplemented with additional training required by staff performing specific data processing roles. Implement processes to confirm that all staff are completing the mandated IG training at induction and on an annual refresher basis including chasing up non-completion.

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 GMP.

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