Northamptonshire Police

Data protection audit report

September 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.

Northamptonshire Police (NP) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 18 May 2020 with representatives of NP to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and NP with an independent assurance of the extent to which NP, 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 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 GDPR and national data protection legislation are in place and in operation throughout the organisation.

Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
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, NP 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 6 July to 23 July 2020. The ICO would like to thank NP for its flexibility and commitment to the audit during difficult and challenging circumstances.

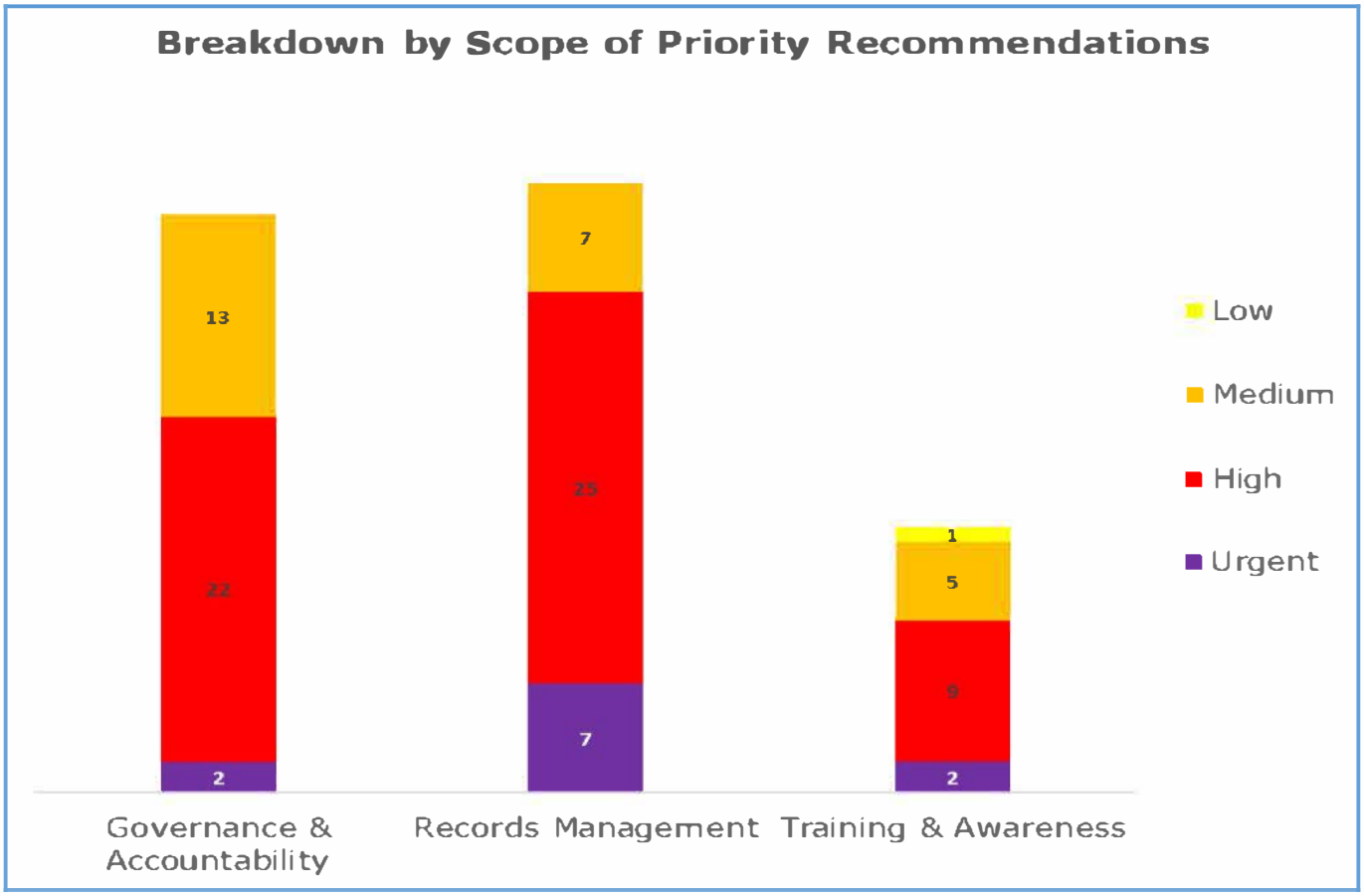
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist NP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. NP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary*

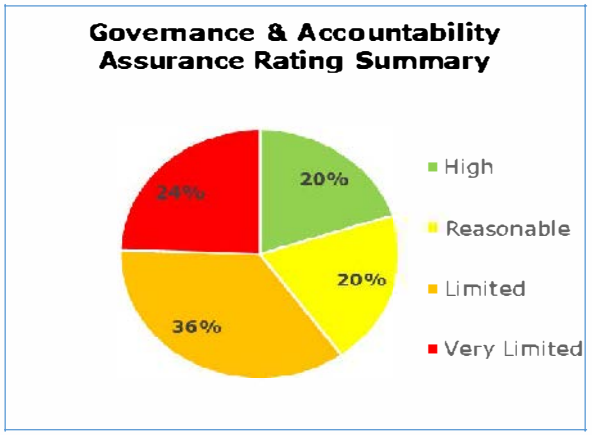
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	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 & 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.

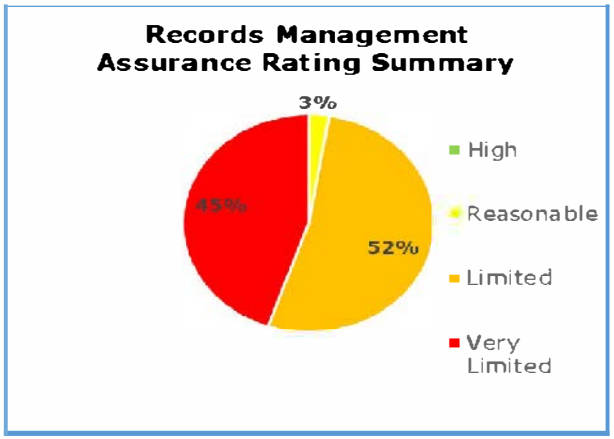
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

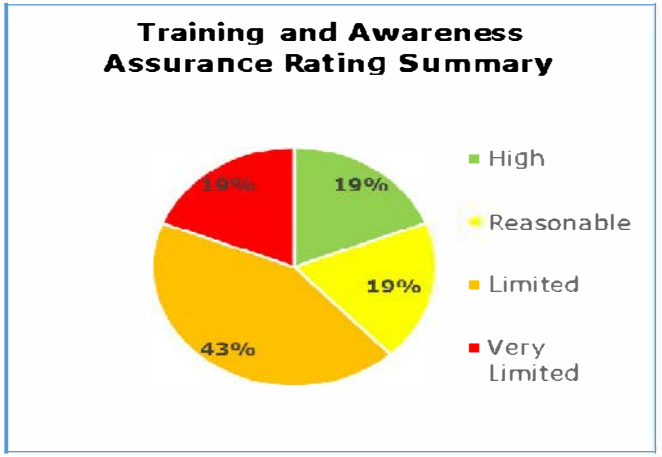
Priority Recommendations



Graphs and Charts







Areas for Improvement

- Complete an information audit/data mapping exercise to create both a Record of Processing Activities and Information Asset Register covering the whole organisation. The exercise is key to comply with Article 30 GDPR and Section 61 DPA18 legislation and establishing the lawful basis for processing personal data/special categories of data.

- Produce comprehensive and clear privacy notices so that individuals are aware why their data is being processed, under what lawful basis (the information audit described above will contribute to this) and what rights they have in relation to that processing.

- The planned recruitment of a dedicated records manager is acknowledged as key to maintain information governance (IG). Support for other IG roles including the data protection officer (DPO), information security officer (ISO) and information asset owners (IAOs) should be reviewed to enable and maintain the appropriate levels of resourcing.

- IG policies and procedures require reviewing to ensure they are up to date with current legislation. They should follow a set format, use appropriate naming conventions, version control and document change history.

- A programme of risk-based IG audits should be initiated as part of an internal audit plan, which should include routine monitoring of any processor acting on behalf of NP. Risk identification and management can be augmented by a regular programme of independent external audits.

- To ensure that manual and electronic records containing personal data are appropriately accessed, classified, stored and disposed of, document formal records management (RM) policies and procedures including sharing personal data with third parties.

- Physical records are not adequately tracked. Without robust tracking procedures in place the risk that the documents could be unlawfully accessed, compromised, or lost is greatly increased. Also, should there be a breach of special category data the harm to the data subject is substantially higher.

- Produce an overall IG training programme policy approved by senior management that incorporates both NCALT national training and needs based training identified for NP staff. Training completion rates should be monitored using agreed key performance indicators (KPIs).

- Develop a Training Needs Analysis (TNA) and an accompanying training plan to identify and address the training requirements of all staff in relation to IG / DP. The DPO needs to have complete oversight of all the training areas and all training content delivered across the Force which include elements of IG.

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 NP.

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