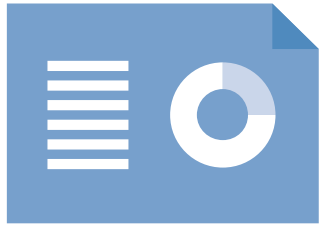
Northumbria Police

Data protection audit report

December 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.

Northumbria Police (NP) agreed to a consensual audit by the ICO of its processing of personal data in December 2019.

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 with Part 3 of the DPA 2018 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.

Information Risk Management	The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of 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, 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 5 October to 16 October 2020. The ICO would like to thank NP for its flexibility and commitment to the audit during difficult and challenging circumstances.

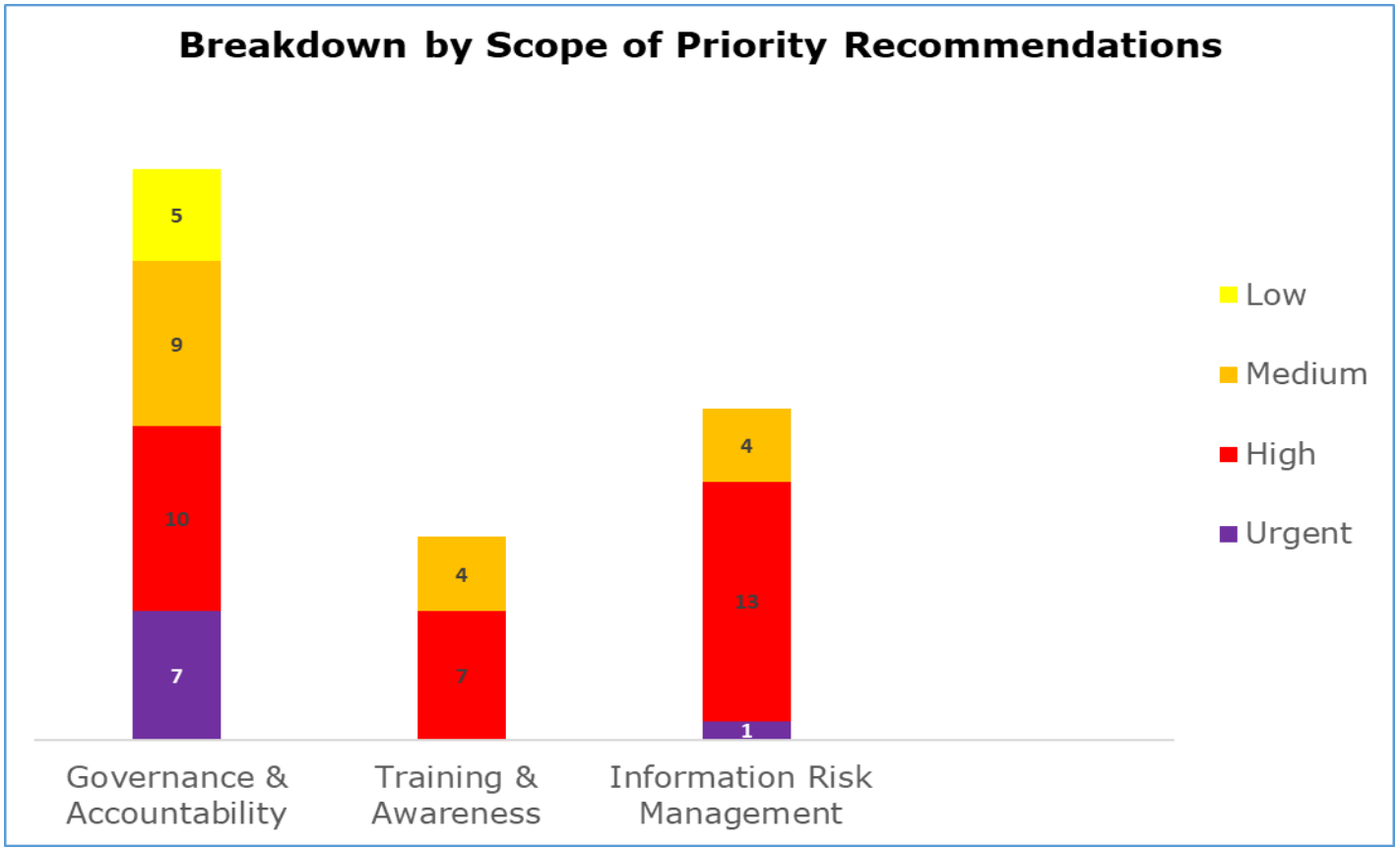
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist NP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are 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*

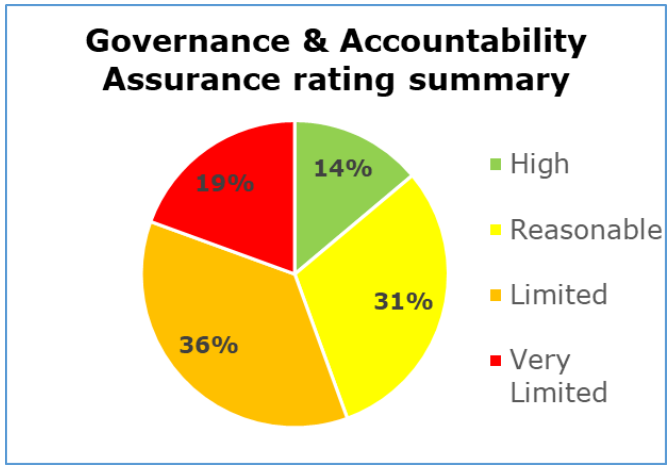
Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to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

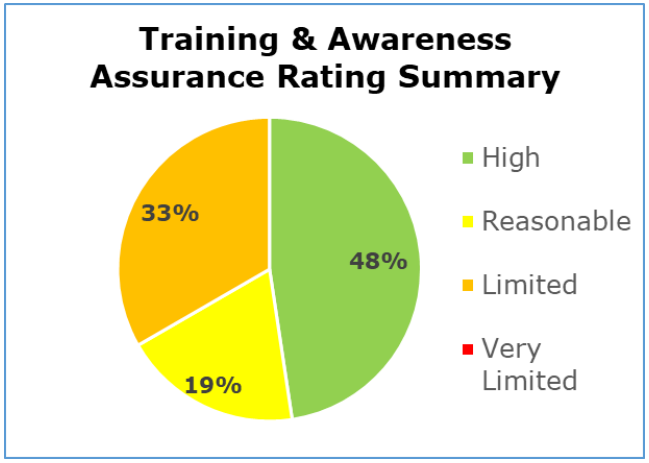
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

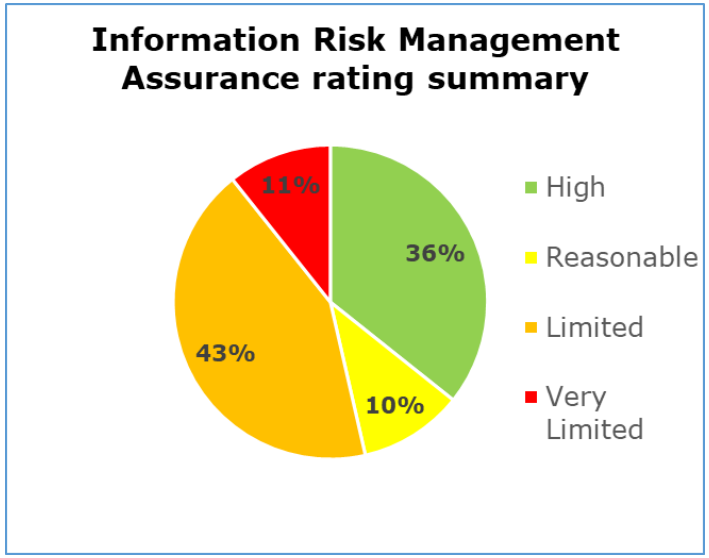
Priority Recommendations



Graphs and Charts







Areas for Improvement

- NP have suite of information governance (IG) policies and procedures, but most do not include sufficient guidance and information relating to the specific requirements for law enforcement processing as detailed in Part 3 of the DPA18. In particular there is no appropriate policy document in place to cover their sensitive processing for law enforcement purposes as required by sections 35 and 42 of the DPA18.
- Internal audits of data protection compliance are contracted to an external provider. The audits undertaken have failed to identify substantial areas of non-compliance with Part 3 of the DPA18. This raises concerns about the external auditor's expertise in relation to law enforcement personal data processing requirements.
- NP has no central oversight of all data processing arrangements which presents a risk that some law enforcement data processor arrangements may not be supported by written contracts as required by section 59(5) of the DPA18. Additionally, NP do not undertake any regular review of data processor contracts or undertake any routine compliance checks to provide assurance that data processors are complying with any data protection terms and conditions in existing contracts.
- NP have recently undertaken a substantial exercise to record all information assets across the force, but this has not included a comprehensive data mapping exercise of their processing activities. This creates a risk that NP lack sufficient understanding of its processing activities to maintain effective oversight and control, including the identification and management of risks. A comprehensive record of processing activity is a requirement of section 61 of the DPA18.
- NP has not properly identified and documented the choice of lawful basis or bases they are relying on from section 35 and Schedule 8 of the DPA18 for its processing of personal data, and sensitive processing to provide assurance that they are complying with the first data protection principle.
- NP has a general privacy notice on its website but there has been no review to ensure that sufficient privacy information is made available in all specific situations. There is therefore a risk that NP are not complying with their obligations under section 44 of the DPA18 and that data subjects may not be aware of their rights and how their information is being processed.
- Refresher IG training should be mandatory on an annual basis as recommended by the College of Policing and completion rates should be accurately reported.

- Adequate training is not in place for staff in specialist roles, such as Information Asset Owners (IAOs), to ensure that they have the knowledge and skills to undertake their role with confidence and reduce the risk of a personal data breach or non-compliance with data protection legislation. This includes training on information risk management and data protection impact assessment (DPIA) completion.
- DPIAs should be assigned a formal review date, or an early review when a substantial change of the process occurs, to allow emerging risks to be identified and mitigating controls enabled. NP should also instigate regular reviews of the implemented DPIA controls to assure they are proving effective.

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.