National Crime Agency

Data protection audit report

November 2022

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.

The National Crime Agency (NCA) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 21 June 2022 with representatives of NCA to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and NCA with an independent assurance of the extent to which NCA, 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 NCA's processing of personal data. The scope may take into account any data protection issues or risks which are specific to NCA,

identified from ICO intelligence or NCA'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 NCA the nature and extent of NCA's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to NCA. It was agreed that the audit would focus on the following area(s)

Scope area	Description
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 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 NCA 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. NCA's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

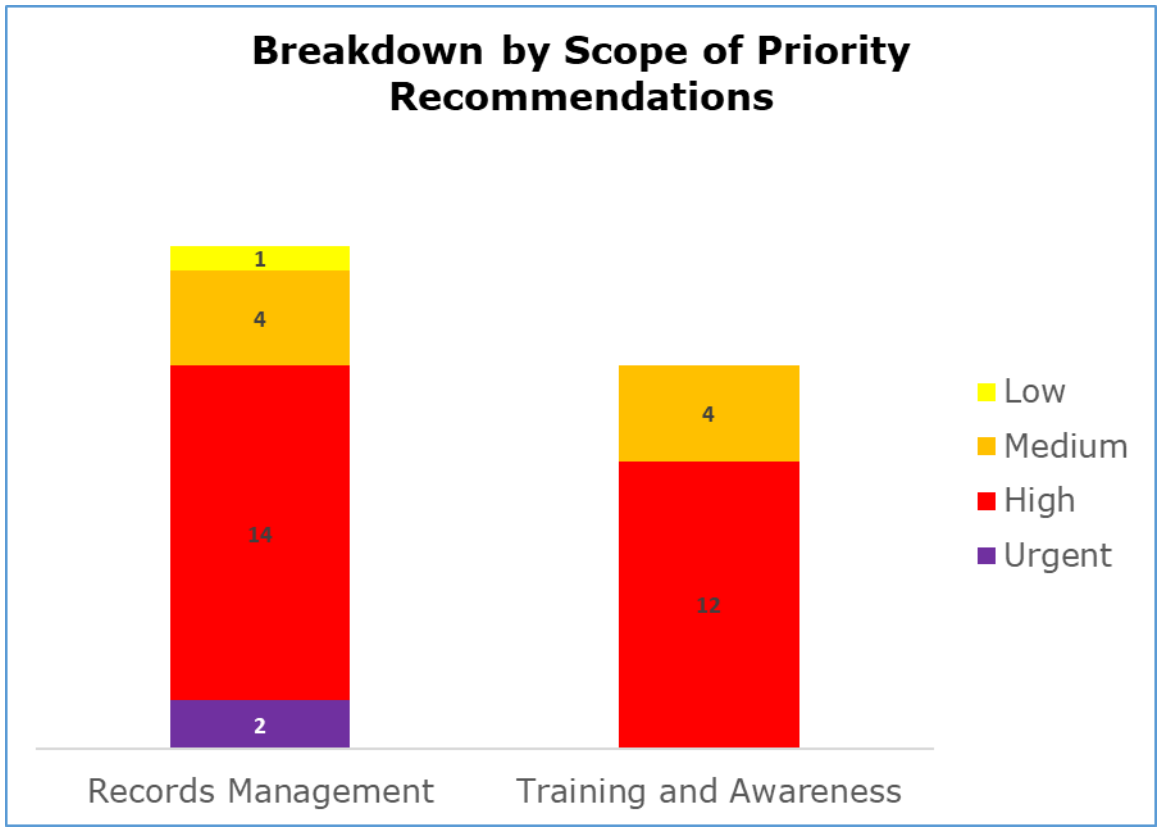
Appendix One - Recommendation Priority Ratings Descriptions.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Records 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.
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 and the rating may not necessarily represent a comprehensive assessment of compliance.>

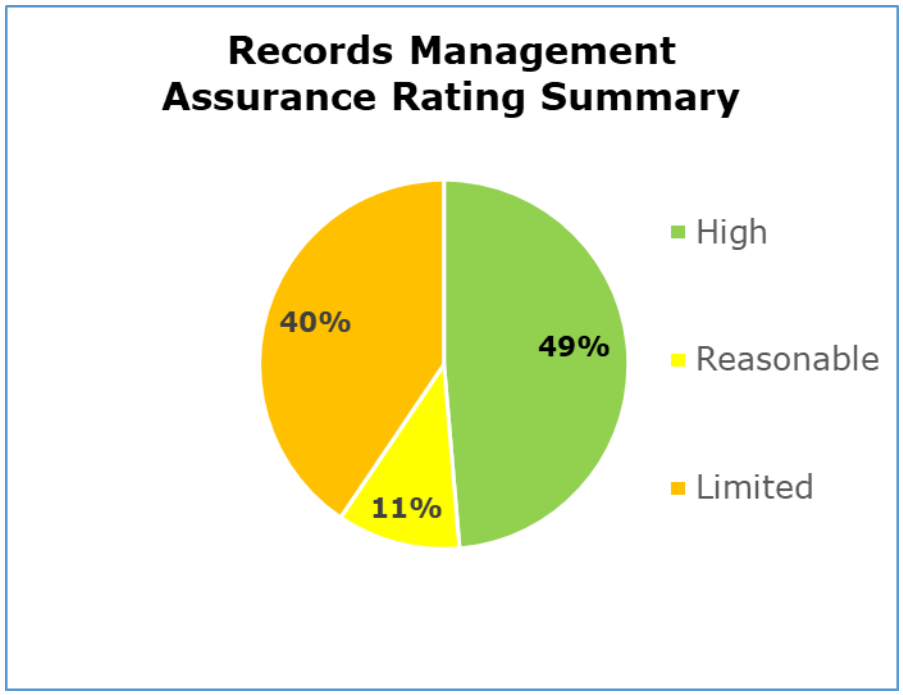
Priority Recommendations



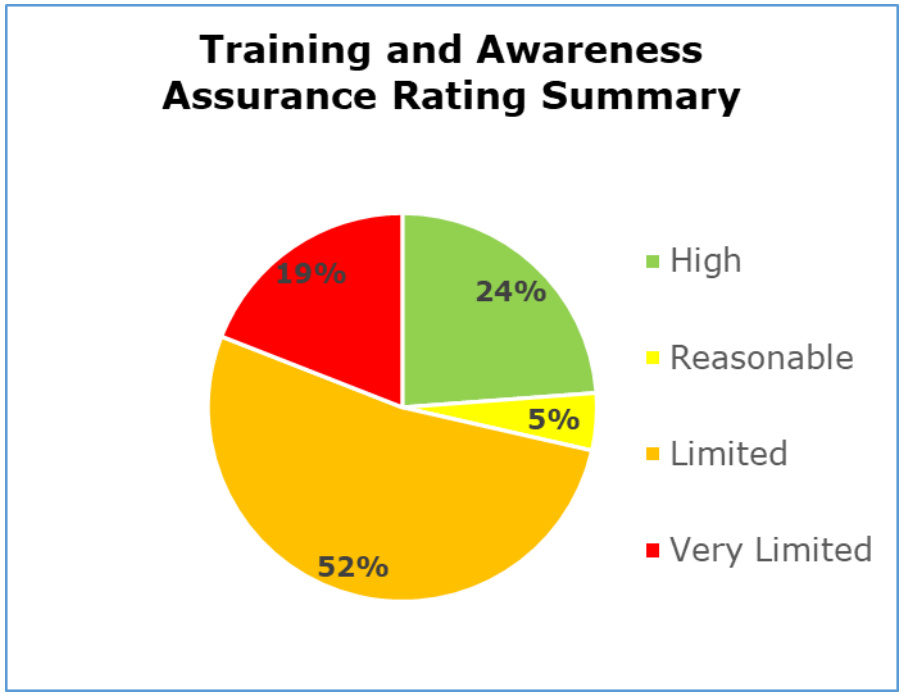
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Records Management has two urgent, 14 high, four medium and one low priority recommendations.
- Training and Awareness has 12 high and four medium priority recommendations.

Graphs and Charts



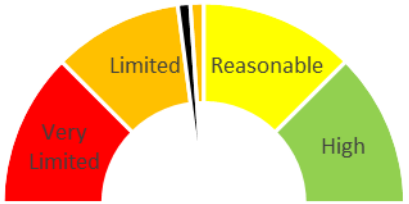
The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 49% high assurance, 11% reasonable assurance and 40% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Training and Awareness scope. 24% high assurance, 5% reasonable assurance, 52% limited assurance, 19% very limited assurance.

Records Management Scope Rating Indicator

Training and Awareness Scope Rating Indicator



The speedometer charts above give a gauge of where the organisation sits on our assurance rating scale from high assurance to very limited assurance.

Areas for Improvement

- Regularly assess the Information Governance (IG) and Data Protection (DP) 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/DP training at induction and on an annual refresher basis including chasing up non-completion.

- Requiring Information Asset Owners (IAOs) to complete an annual checklist will assist NCA in completion of an information audit/data mapping exercise. This would ensure that all data processors are clearly identified and create both a complete Record of Processing Activities (RoPA) and Information Asset Registers (IARs), to incorporate all business areas across NCA. The exercise is key to comply with Article 30 of the UKGDPR and section 61 DPA18 legislation and establishing the lawful basis for processing personal data, special categories and sensitive processing of data.

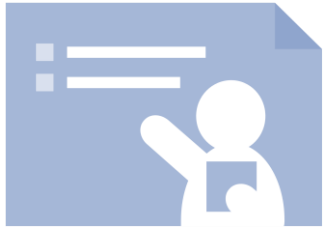
- Further detail in the NCA privacy notice on the parties that data is shared with and reference to specific retention periods will assist NCA to meet with the requirements of Articles 12 and 13 of the UKGDPR and section 44 DPA18.

- Regular weeding alongside review, retention and disposal of physical and electronic records in line with their retention schedule will ensure that NCA are not keeping personal data for longer than is necessary.

- Tightening procedures around staff transferring roles within NCA will assist with access control and ensuring staff only have access to systems and areas containing personal data that they are authorised to.

- Logging of automated law enforcement processing systems (any IT database) needs to be completed for all NCA systems to meet section 62 of the DPA18 requirements.

Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations – These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to 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 the National Crime Agency.

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