ICO Audit: a year in focus

2022/2023

Information Commissioner's Office

Foreword

Regulatory Assurance' purpose is to enable those responsible for processing personal data to do so with increased regulatory certainty and in compliance with information rights legislation.

This is a year in which we hit incredible heights in terms of the numbers of audits and follows up completed and of audit recommendations accepted and actioned. From April 2022 to April 2023 a total of 71 audits were completed, involving over 1280 hours of audit interview time, a 48% increase in audits completed compared to the previous year. This was at a time when organisations were emerging from the effects of the global pandemic and where remote working continued, creating continued challenges to our business-as-usual working processes and plans.

2022/23 was the first year since the Covid pandemic when we have been able to audit without restrictions but with continued use of the offsite techniques developed during lockdown. With just under three quarters of our work delivered offsite, we have been able to reduce the number of auditors assigned to each audit while increasing the number of audit hours. It is our intention to move to a hybrid approach in the coming year with more balance between onsite and offsite work.

Our impact is greater than the numbers we achieve, the impact of our action can be seen in the audit programmes we have undertaken this year. Whether that be the work we did to assess the compliance of Scottish Government departments and Scottish NHS Boards or new challenges with the audits of gaming designers' conformance with the Age Appropriate Design Code.

Over 96% of organisations audited stated that the audit met their expectations in terms of what they were looking for and received from the ICO, which is a positive indication of the real benefit of our audits to organisations and the reputation of the ICO as an empowering regulator providing regulatory certainty.

This report conveys the scale and breadth of the work the team has undertaken this year by outlining some of the key themes we have seen during our audits in terms of good practice and opportunities for improvement; and the impact we have made.

Ian Hulme
ICO Director of Regulatory Assurance

Background

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers. 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.

This report is based on our findings from our audits over the last year, focussing on the key themes identified, the recommendations we've made and the good practice we've seen. We are sharing these findings as part of our commitment, under our ICO25 strategic plan, to act as a 'hub' for good information rights practice. Organisations can access real-life examples of what the law requires and what good looks like and benefit from the advice and support of the regulator when planning, innovating and managing information risk.

What we've done

From April 2022 to April 2023, the ICO audit team completed 71 audits and 25 audit follow up reviews. This represents a 48% year on year growth in audits completed compared to 2021/22.

The audits were split across the following sectors:

- 22 health sector audits, primarily of the Scottish Health and Territorial or Special Boards.
- 12 criminal justice sector audits.
- 11 audits of the private sector which mainly consisted of audits under the ICO's Age Appropriate Design Code (the code).
- Nine central government audits under the Digital Economy Act 2017.
- Six audits in the public sector in Scotland.
- Five audits under the Investigatory Powers Act.
- Two local authority audits and two in the charity sector.
- one audit in the education sector and one audit of a private insurance organisation.

In addition, the team have completed bespoke audit engagements and project work covering:

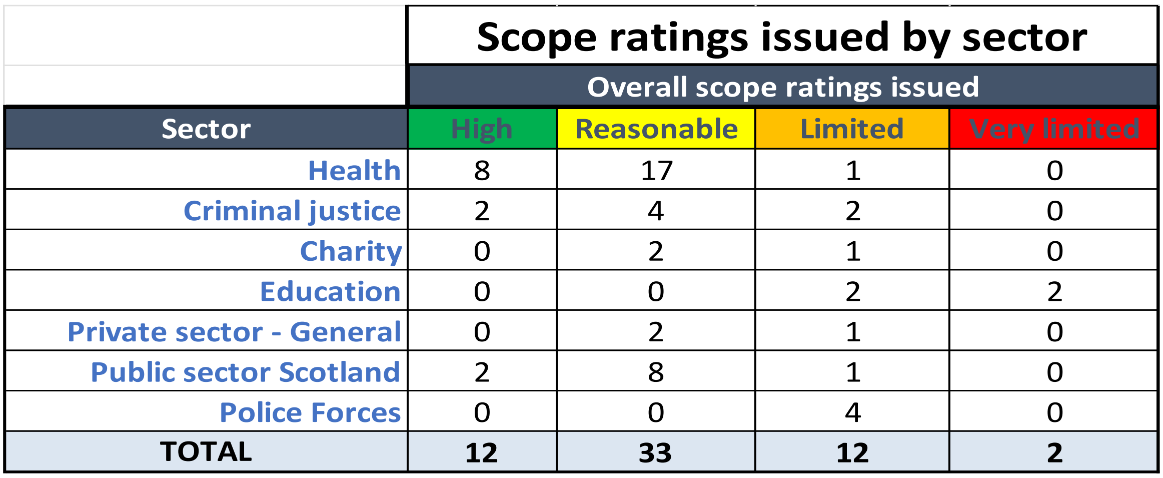
- Artificial Intelligence
- Part 3 DPA 2018 s.62/Key Stroke Monitoring/Employee Surveillance
- AdTech – audits looking at Data Management Platforms

- The Network and Information Systems Regulations 2018 (NIS) audits – development of a framework to facilitate compliance assessment audits of the relevant digital service providers in scope of the Regulations.

What we’ve found

When conducting an audit, we assess the arrangements an organisation has in place for complying with data protection legislation and the extent to which they are being adhered to.

We then give an overall rating to show whether the key risks to non-compliance are being managed effectively. The table below shows the assurance ratings that we have given by sector[1].



	Scope ratings issued by sector			
	Overall scope ratings issued			
Sector	High	Reasonable	Limited	Very limited
Health	8	17	1	0
Criminal justice	2	4	2	0
Charity	0	2	1	0
Education	0	0	2	2
Private sector - General	0	2	1	0
Public sector Scotland	2	8	1	0
Police Forces	0	0	4	0
TOTAL	**12**	**33**	**12**	**2**

It is encouraging that there were only two very limited assurance (red) ratings awarded in any scope areas, both of which were in the education sector.

20% of assurance ratings awarded were high assurance, meaning there was a high level of assurance that processes and procedures were in place and were delivering data protection compliance in these scope areas. The health sector saw a high proportion of high assurance ratings awarded which were centred around our work with the Scottish Health and Territorial Boards.

In most sectors, the main rating given was reasonable assurance[2].

[1] See Appendix 1 for assurance rating descriptions

[2] It is worth noting that certain bespoke audit engagements were not assessed under our standard assurance rating process and so are not represented in the figures above.

What we’ve recommended

Audit recommendation figures

We made over 1500 recommendations in total during the year of which over 99% were accepted or partially accepted.

Audit recommendation themes

The most common recommendations made in our consensual audits were:

Documenting processing activities
Organisations should complete a data mapping exercise across the business to understand the processing activities taking place. This will help ensure the Record of Processing Activities (RoPA) includes key elements such as what type or types of personal data is being processed; whether any special category data is present; where the data came from; and the lawful basis for any data sharing that takes place as part of the process. Organisations should repeat this mapping exercise periodically to enable them to review their RoPA entries on a regular basis.

Completing Data Protection Impact Assessments (DPIA)
Organisations must improve current DPIA processes to include legislative requirements such as external stakeholder, data processor and DPO consultations; and guidance on how staff should act on the outputs of the DPIA (including recording risks on relevant risk registers). Creating ‘screening templates’ will prompt the documentation of these consultations and the decisions taken as a result. It is important to have a process to inform the ICO when residual high risks have been identified that cannot be mitigated before processing takes place.

Providing privacy information
Organisations must review and enhance existing privacy information provided to people to ensure it includes all the requirements of the UK GDPR. Privacy information should be available in different languages, formats and for different society groups such as children and vulnerable adults to ensure transparency without discrimination. Implementing periodic reviews of all privacy information will ensure that it remains up to date and relevant.

Embedding privacy management frameworks
Organisations should make improvements to existing privacy management frameworks and policies to document reporting lines and how information flows between senior management, governance boards and those with specific data protection responsibilities. Information governance roles and responsibilities should be correctly assigned and accurately reflected in job descriptions; staff in

these roles should have sufficient protected time so that privacy work is carried out effectively. Having formal governance steering groups or committees will help oversee data protection compliance across the organisation.

Delivering training
Organisations should conduct a role-based training needs analysis to identify training requirements for all staff and those with specific data protection responsibilities. Giving specialised training to those in key roles will help support the governance framework and data protection compliance. By specifically including key elements of FOI/EIR in induction training and providing refresher training will help maintain knowledge and awareness in this area.

Sharing data
Data sharing agreements must include appropriate data protection and security clauses and details of how individual rights requests will be managed. By keeping agreements under regular review, particularly when a change of processing activity or legislation takes place, will provide ongoing assurance on the legality and appropriateness of the data sharing.

Using data processors
Organisations must ensure that all data processors are identified and that an appropriate contract is in place that sets out the details of the processing. Prior to entering into a data processing arrangement organisations should complete appropriate due diligence checks, including a security review. Periodic compliance assessments of contractual arrangements should be scheduled and completed during the contract lifecycle to provide assurances that contract arrangements are being met.

Challenging recommendations

When we asked organisations which recommendations they found the most challenging to implement and why, they said:

- "Updating supplier contracts - the nature of our organisation means there are thousands!"
- "Pinning down the minutiae of consent v law enforcement purposes and assisting the organisation to understand this."
- "Structuring a layered privacy notice in an organisation with many, many functions and operations."
- "Role profile changes and a departmental restructure which was challenging but was achieved with very little additional budget. However, the requirement for data protection audits has proved more difficult to achieve which was simply down to lack of funds."
- "Completing the ROPA and data flow mapping."

- “Increasing resources to process SAR's due to budget pressures in Local Government.”
- “System changes that rely on the system having the capability to do things. Some of those things weren't possible with the current technology.”
- “Actions that needed a change in culture and practice which affected the whole organisation.”

We believe that the opportunity to speak to our audit teams was of real benefit to the organisation in understanding what was needed and thinking of solutions to these challenging recommendations.

Good practice

Throughout the year we were encouraged to see some good practice in some of the organisations that we audited. Examples of this good practice included:

- The use of a comprehensive processor contract performance tracker to manage and risk assess all contracts. This provided assurance that data processors and third-party suppliers continued to perform at the expected service level and that new risks to personal data or organisational security were identified.
- The inclusion of an assessment of the privacy risks as a result of any automated decision within a DPIA template to ensure the impact of this type of processing activity could be better understood and any risks considered and mitigated.
- The development and publication of a range of supplementary privacy information to improve transparency of specific data processing activities, including privacy information specifically for children which explains how their data is used in a clear, understandable and accessible format.
- The introduction of a bespoke central system for recording processing activities and completing DPIA, Data Sharing Agreements and other compliance documents. The system automatically provided staff with relevant forms based on their screening responses and reminded key stakeholders when documents were due for regular review. This helped to give assurance that assessments were being completed when required and were being updated with relevant information when necessary.

What we’ve changed and the impact we’ve made

Customer service standards

We measure how we have influenced change within an organisation, and how our work has benefited the organisation and added value through the audit process. This is identified through our follow up work. In 2022/23 we found that 96% of the original recommendations accepted by the organisations audited had been (or were in the process of being) actioned by the time of the follow up.

The data demonstrates that the team are influencing real measurable change in organisations’ compliance with data protection legislation and promoting a positive message on the benefits of adopting a privacy by design approach.

Impacts made by our bespoke audit work

Impacts to children’s privacy online
Examples of changes seen and evidenced within the gaming industry in relation to the protection of children online, as a result of ICO audit engagement, included:

- Specific child privacy checkpoints built into the game development process, where compliance and risks are assessed and a go/no go decision is taken for the whole project based solely on the code’s criteria.
- Development of a suite of guidance for parents and guardians about gaming products. Namely how children interact with those products, what the potential risks to those players may be, and linking to relevant third parties who can provide additional support.
- Wide ranging and extensive market research being undertaken to develop a thorough understanding of the age demographics of the player base, in a privacy respecting fashion, then exploring different age assurance solutions that could provide greater level of certainty compared to a declarative approach.
- Publication of detailed internal guidance for technical and operational staff on how the code applies to their work, to ensure that there is never any doubt or confusion, and that there are clearly established escalation routes within the organisation in the event of any problems.
- ‘Risky’ features within products and services including chat, friends lists, push notifications and social features for U18s in the UK disabled by default to support the best interests of children.

This work culminated in the publication of top tips for the gaming industry to educate the sector in the importance of children's privacy and give practical advice on steps that can be taken to achieve this.

We also developed a risk tool for use more widely by providers of online services to enable them to conduct their own self-assessment of the risks within their product or service and action plan mitigating measures to improve the protection for child users.

Digital Economy Act review outcomes

During our reviews, we were struck by the enthusiasm of the participating organisations. All organisations were keen to know what they had done well, and how they could improve. The feedback we received has reflected the positive nature of their experiences. In particular they reported that;

- the reviews helped them understand their key risk areas with regards to their data sharing activities; and
- the recommendations we made were constructive and appropriate.

We supported the compliance teams in each organisation at an operational level as part of their continuous improvement cycle. We took account of their registers of risk, action plans and associated management information. This information, together with our review findings and action plans, helped us understand how they had improved their practices when we followed up on our work.

In our follow up engagements, we reviewed how participants implemented our recommendations and identified if they needed any further advice. In most cases, the organisation had already implemented most of our recommendations, before we followed up with them. We have not found it necessary to take any regulatory action in relation to any of the participants reviewed. Our outcomes report is available on our website.

Impact to service users following our voluntary compliance work with the Department for Education (DfE)

As a result of our engagement with the DfE, below are a sample of improvements planned or implemented that will have a positive impact on service users in the future.

- DfE continue to review and update privacy information to improve usability and ensure the information is user/child-friendly and suitable for all DfE's audiences or stakeholders.
- Closer working relationships continue to evolve with the educational sector to ensure children's information rights and wellbeing are considered when

handling information requests that the department receives from parents or guardians.

- There is a planned production of an Information Rights code of practice for use by education establishments.
- The 'Data Protection Portal' aimed at learners, parents/ carers, and education staff was launched in February 2023. It contains data protection learning & training materials, deep dives on the use of data in DfE projects, a comprehensive index of data protection information for data subjects and more. It will available online for anyone to access – including DfE staff so there is a consistent understanding across the DfE and the sector.
- They have implemented a new DfE (& Executive Agencies) Data Sharing Service with clearer roles and responsibilities, more effective principles, processes and procedures and a new suite of forms and guidance documents.

What value we added

Feedback evidence

Immediately following an audit we ask for feedback on the audit engagement.

In the overwhelming number of cases, organisations were happy with the audit engagement process and the professionalism of our team. They agreed with the scope of the audit and with the assurance ratings we awarded. Over 96% stated that the audit met their expectations in terms of what they were looking for and received from the ICO. This is a positive indication of the real value in our audits and enhances the reputation of the ICO as an empowering regulator.

Some of the positive comments made included:

> "A very worthwhile experience with very knowledgeable staff."
>
> "We thought your audit was really well conducted and we received very positive feedback from our staff who met with the assessor."

Some constructive anonymised comments made included:

"The audit was professional and staff courteous and business like at all times. A potential improvement would be for a more detailed response in the written report on the audit actions including areas that the organisation did well, which was touched on but as the report was largely an exception report it mainly highlighted areas for improvement, and also the scoring criteria."

“My only reflections are around the volume and depth of recommendations and subsequent activity required. I feel had we known then we would have sought to agree further time to work on the action plan from the start and would have avoided the request for an extension. Perhaps consideration could be given as to how this can be flexible in future, given the operational nature and demand on (operational) functions coupled alongside the planning and demand of the Audit Team also.”

Once organisations have had time to work on their actions to address our recommendations we ask for feedback on the overall impact of the audit engagement.

The feedback suggests that one of the key impacts of our audits is that they raise data protection awareness within the organisation at all levels and particularly with senior leadership teams.

Over 73% of respondents stated that the data protection culture across the organisation had improved as a direct result of the audit. This demonstrates how our audits can empower and motivate organisations to strengthen their approach to data privacy and provide regulatory certainty that measures they have or will implement following our recommendations will be effective.

Positive feedback comments included:

“The overall process was extremely supportive and provided us with improved knowledge and awareness of Data Protection legislation. As an NHS organisation, we are used to complying with the standards set out in the Data Security and Protection Toolkit, but there are key elements of legislation that are not included in this assurance tool. Therefore the opportunity provided by the ICO was very valuable.”

“I thought the process was really useful to increase the robustness of information governance documentation and it also assisted with senior management buy in.”

“It was a very useful experience, which help provide a focus for change and improvement, in our processes and our thinking.”

Constructive suggestions for additional improvements to process included:

"For a consensual audit and one which required a lot of work for us, we would have liked a bit more flexibility on agreeing the scope areas. More direction up front about matching interviewees to controls to be tested would have been helpful. We felt there was a varying degree of value to the recommendations, a few felt quite trivial. Would have liked more emphasis on the things we were doing well and more detail on which controls were assessed as reasonable or high assurance."

"From a guidance perspective it would be good if the ICO could work more closely and assist in how we could actually meet their expectations. For example - data flow mapping - tell us how we could do that and how this recommendation could be met."

What's next

New proposed areas of work for 2023-24

ICO25 - The use of Artificial Intelligence (AI) in recruitment
To undertake a programme of consensual audits and engagements with both providers and users of AI systems for the purposes of recruitment.

ICO25 - Financial services
Gather intel to develop a programme of reviews looking at various themes that are of interest to the ICO, such as data protection compliance and where this fits across addressing financial or economic crime; developing new technologies, innovative products and business models; regulatory co-operation; international finance, and regulation.

ICO25 - Data sharing in child protection/safeguarding project
Programme of work across the multiple agencies/sectors, who are responsible for child safeguarding (local authorities, social services, education, police, health) to identify any weaknesses in current arrangements and see where we might be able to provide guidance or clarity to increase their effectiveness.

Mobile Phone Extraction
Assessment of compliance with data protection legislation with regards to the extraction and use of mobile phone data in criminal investigations by the criminal justice sector.

Privacy & Electronic Communications Regulations audits
Conduct audits of public electronic communications network / service providers.

Appendix 1 – Assurance rating descriptions

Ratings and statistics

Where appropriate, each scope area covered in our audits is rated using the following four assurance levels:

High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
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.
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.
Very Limited	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.