A guide to ICO audits

Information Commissioner's Office

Contents

Executive summary

The Information Commissioner has identified audit as having a key role to play in educating and assisting organisations to meet their obligations. As such, the Information Commissioner's Office (ICO) undertakes a programme of consensual and compulsory audits across the public and private sector to assess their processing of personal information and to provide practical advice and recommendations to improve the way organisations deal with information rights issues.

S146 of the Data Protection Act 2018 contains a provision giving the Information Commissioner the power to carry out investigations in the form of compulsory data protection audits, but we predominantly conduct consensual audits under the provisions of s129 of the Data Protection Act. These audits are completed by our Assurance department.

Audit allows us to assess any organisation's processing of personal data for the following of good practice. The executive summary for each audit is published on our website which shows the high level findings and assurance ratings for the scope areas audited.

The benefits of an audit include:

- helping to raise awareness of data protection, general information security and cyber security;
- showing an organisation's commitment to, and recognition of, the importance of data protection and individual rights;
- having high levels of personal data protection compliance helps organisations innovate and deliver great services by building trust with the public and consumers;
- the opportunity to access ICO's resources at no expense;
- independent assurance of data protection policies and practices;
- identification of data protection risks and practical, pragmatic, organisational specific recommendations to address them;
- the sharing of knowledge with trained, experienced, qualified staff and an improved working relationship with the ICO; and
- enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

The focus of an audit is to determine whether the organisation has implemented policies and procedures to manage the processing of personal data and whether that processing is carried out in accordance with such policies and procedures. When an organisation complies with its

data protection requirements, it is effectively identifying and controlling risks to prevent data protection breaches.

An audit will typically assess the organisation's procedures, systems, records and activities in order to:

- ensure that appropriate policies and procedures are in place;
- verify that those policies and procedures are being followed;
- test the adequacy of controls in place;
- detect breaches or potential breaches of compliance; and
- recommend any required changes in control, policy and procedure.

The scope areas to be covered during the audit will be agreed, in consultation with the organisation, prior to the audit. The scope may take into account any data protection issues or risks which are specific to the organisation, identified from ICO intelligence or the organisations own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely.

The ICO will make recommendations to assist organisations to mitigate the risks of non-compliance, and reduce the likelihood of damage and distress to individuals and regulatory action being taken against the organisation for a breach of data protection legislation.

Following completion of the audit the Assurance team will provide a report that gives an assurance rating for each scope area covered; observations and findings that focus on the areas of weakness and greatest risk or areas of particularly good practice that have been identified; and priority-rated recommendations to address the weaknesses and risks. We will also provide an executive summary of the report. The audit process provides an opportunity for the organisation to respond to observations and recommendations made by the audit as the action plan is drafted. An executive summary of the final report is published on the ICO website.

Compulsory Audits

Whilst we predominantly conduct consensual audits, the ICO also has the power to conduct compulsory audits, under s146 of the Data Protection Act 2018. This power allows the ICO to issue an 'assessment notice' and require a controller to allow us to evaluate their compliance with data protection legislation. More information about our use of assessment notices can be found in the Regulatory Action Policy.

1. Audit programme development

Audit planning and risk assessment

The Information Commissioner has adopted a risk-based, proportionate and targeted approach to audit activities and follows a by-exception approach to reporting.

To identify high-risk controllers and sectors the ICO uses a number of sources, including:

- reported breaches
- the number and nature of complaints received by the Information Commissioner;
- controllers' annual statements on control and other publicly available information;
- business intelligence such as media reports and;
- other relevant information.

From this risk analysis work a programme of audits will be developed. Controllers volunteering for audit will also be considered for the programme in line with the risks that their processing activities raise and subject to resource availability.

Audit planning and risk assessment for individual organisations will be based on the potential impact or likelihood of risk to freedoms and rights of individuals. And in determining this one or more of the following factors will be considered:

- the compliance 'history' of the controller, based on complaints made to the Information Commissioner and the controller's responses;
- 'self reported' breaches and the remedial actions identified by controllers;
- communications with the controller which highlight a lack of compliance controls and/or a weak understanding of data protection legislation;
- business intelligence, such as news items in the public domain which highlight problems in the processing of personal data by the controller, and information from other regulators;
- statements of internal control and/or other information published by the controller which highlight issues in the processing of personal data;

- internal or external audits conducted on controllers related to data protection and the processing of personal data;
- data protection fees and history;
- the implementation of new systems or processes where there is a public concern that privacy may be at risk;
- the volume and nature of personal data being processed;
- evidence of recognised and relevant external accreditation;
- the perceived impact on individuals of any potential non-compliance; and
- other relevant information e.g. reports by 'whistleblowers', and data protection impact assessments carried out by the controller.

In determining the potential impact of non-compliance on individuals the following are taken into consideration: the number of individuals potentially affected; the nature and sensitivity of the data being processed and the nature and extent of any likely damage or distress caused by non-compliance.

As well as proactively approaching organisations identified through the risk assessment process, there are a number of other potential sources of audits:

- organisations which volunteer for, or request, audits;
- those identified as potentially benefiting from an audit by other ICO departments, in particular the regional offices and our Policy, Intelligence and Engagement Teams; and
- those identified through investigations conducted by our Enforcement Team.

These organisations are also considered on a risk basis and are assessed based on the factors outlined above.

2. Audit approach

Once the audit has been confirmed an introductory meeting or conference call will be arranged to discuss the audit process. Specific dates for each element of the audit will be agreed; we will work with organisations to minimise the impact on their day-to-day work as far as possible. A draft letter of engagement will be used as an agenda at the introductory meeting to develop the scope of the audit and set appropriate timescales.

At the introductory call the audit scope will be agreed, in consultation with the organisation; it will consider any current known risks, generic data

protection issues, as well as any organisation specific concerns there may be about data protection policies and procedures.

The scope areas that may be covered include:

- data protection governance and accountability;
- staff data protection training and awareness;
- security of personal data;
- individual rights requests;
- information sharing;
- records management; and
- Data Protection Impact Assessments and information risk management.

Prior to the introductory meeting the audit team will liaise with ICO colleagues to gain background and contextual information on general themes/complaints about the organisation that may affect the scope of the audit.

Within a few days of the introductory meeting, we will issue a formal letter of engagement to reflect the discussions and agreed scope of the audit.

Document review

Prior to the audit we will request necessary policies and procedures that relate to the agreed scope areas from the organisation being audited. These may include data protection policy documents; operational guidance or manuals for staff processing sensitive data; data protection training modules; risk registers; information asset registers; information governance structures, records of processing activities and similar. These documents will be used to inform the direction of the audit and are reviewed at the ICO's offices prior to the scheduled audit dates.

Key personnel may be interviewed prior to the scheduled audit dates, to further assess the design effectiveness of controls the organisation has in place. We may also ask for operational data and KPIs used to manage SLAs or performance to gain an understanding of adherence to process.

The audit

The ICO will make use of remote techniques and conduct interviews where auditing virtually is suitable. Some of the benefits of this approach are being able to view and share screens, review work as it happens and

conduct interviews with a high degree of flexibility as well as interview in many locations and settings.

The first day will begin with an opening meeting, attended by appropriate members of the operational and senior management team of the organisation, to discuss the process and practical considerations. This provides an opportunity to discuss any issues and answer any questions that the organisation may have about the process.

Ahead of the audit, we will work with the organisation to ensure that the audit will be productive by identifying appropriate key members of staff to interview and relevant processes to test and examine. These interviews will be agreed in a schedule, drawn up by the organisation in consultation with the audit team.

During the audit the team will primarily conduct individual interviews with key staff or subject matter experts in the scope areas agreed. We will aim to see how processes and policies work in practice to assess their operational effectiveness. These interviews will be supplemented by potential data analysis, reviewing KPIs and examples of selected processing of personal data within the organisation and, where appropriate, testing of controls. During the interviews all auditors will make notes of their findings from interviews, observations and testing.

The questions asked, and evidence gathered, will depend on the scope areas agreed and listed in the letter of engagement. However, there are some generic areas such as the governance structure that is covered on each audit.

If during the audit we identify a data breach (for example, a reportable incident, that hasn't been reported to the ICO) we'll inform the organisation of the finding as soon as practically possible, explain what actions need to be taken and what the next steps will be from the ICO's perspective.

In order for the audit to be effective the ICO will require access to key documents, records and systems and questions posed by the audit team should be answered comprehensively and accurately.

At the end of each day, the audit team will highlight any areas of concern that have arisen to their point of contact within the organisation, to give the organisation the opportunity to conduct further investigations or provide further evidence whilst the audit team are still directly engaged.

Upon completion of the scheduled interviews, the audit team will hold a closing meeting with the organisation's key stakeholders. If any major concerns have been identified by the audit team, they will be highlighted

at this point. As far as possible, a general overview of the audit progress and what happens next will also be covered. Also at this point the lead auditor will explain the approximate timescales for any potential follow up activity.

Draft and final reports

As detailed in the letter of engagement, a draft report will typically be issued within 10 working days of the scheduled audit days. The report will:

- provide an assurance rating for each scope area;
- detail non-conformities and associated risk and;
- include prioritised recommendations that may mitigate risks.

The organisation will be required to accept, partially accept or reject the recommendations and complete an action plan indicating how, when and by whom the recommendations will be implemented. The final report will then be issued and an executive summary published.

By its very nature a two or three day inspection of an organisation processing a substantial volume of personal data cannot be deemed to be conclusive. Final report findings and recommendations should always be viewed in this context and are unique to the organisation. It is a matter for the ICO to determine the content of the final report, and it is indicative of the level of assurance regarding an organisation's policies and procedures in respect of the data protection regulations at a certain point in time, in relation to the agreed scope areas.

Publication

After an audit we will publish the executive summary on the ICO website.

3. Audit follow-up

The audit team will be in touch to arrange any follow-up activities which will be agreed at the end of the audit. A follow-up audit is where an organisation shows the ICO work done towards the agreed recommendations following the original audit. We will pay particular attention to ensuring that urgent and high priority recommendations have been (or are being) addressed. Where they are not, we may consider further action in line with the ICO's Regulatory Action Policy.

For completed follow-ups a report for the organisation will be produced, however, we do not publish the follow-up executive summary, but instead will add a short statement on the website to notify that we have undertaken follow-up work.

4. Frequently asked questions

Will it take a lot of time?

We try to keep the disruption to the organisation to a minimum. We use a single point of contact, agree timings with the organisation and ask them to provide a schedule of interviewees. Typically, the audit will be no more than a week and dates to produce the reports are agreed in the letter of engagement.

How much will it cost?

An ICO audit is free.

Will we be able to feedback to the ICO about the audit?

In order to ensure that our processes are relevant and efficient we will issue feedback questionnaires to the organisation after each audit. The ICO will use this information to improve our procedures and inform subsequent audits.

Will you always publish the report?

An executive summary will be published, and this high-level document contains only the background to the audit, the overall audit opinion the areas of good practice and those areas needing improvement. The detailed findings are not published.

What about confidentiality?

Any member of the ICO is legally bound, under section 132 of the DPA 18 not to disclose any information given under a duty of professional secrecy.

What about enforcement action?

The Information Commissioner sees audits as a positive and educative process to support conformance to data protection legislation as well as encourage good practice.

However, on the rare occasion and depending on the type and severity, the Information Commissioner reserves the right to utilise its enforcement powers when a serious non-compliance is discovered during an audit.

Are the team qualified?

The ICO audit team all undertake internal audit training on induction, and thereafter may take or work towards the ISO27001:2013 Information Security Lead Auditor qualification, which is the industry standard for information security. They may also have a range of skills and backgrounds including data protection casework, quality management, business improvement, policing, the banking sector, IT services and financial audit.

Can organisations request an audit?

Yes. Each year we conduct a number of audits with organisations who have approached us and who would like to benefit from the knowledge and skills of the team. We do, however, take a risk-based approach in prioritising organisations.

Is other legislation audited?

We do audits of the Data Protection 2018 Legislation, Privacy and Electronic Communications Regulations (PECR), Freedom of Information Act (FOIA), the Investigatory Powers Act (IPA) and also where information rights overlap with other legislation such as the Digital Economy Act (DEA).