A guide to ICO audits

Information Commissioner's Office

Contents

Executive summary

The Information Commissioner, who is responsible for enforcing and promoting compliance with the General Data Protection Regulation 2018 (the GDPR), 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.

Article 58.1(b) of the GDPR 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. 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. This includes, but is not limited to, compliance with the requirements of the GDPR and may also include Freedom of Information rights. 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;
- 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; and
- the sharing of knowledge with trained, experienced, qualified staff and an improved working relationship with the ICO.

The focus of an audit is to determine whether the organisation has implemented policies and procedures to regulate 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 personal data 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.

Whilst we predominantly conduct consensual audits, the ICO also has the power to conduct compulsory audits, under article 58.1.b of the GDPR. This right extends to any public or private organisation and in the form of a compulsory 'assessment notice' to evaluate their compliance with the data protection principles.

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. Data 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 eg 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 and Engagement Team; 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. Provisional dates for the audit site visit will be agreed; we will work with organisations to 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 (see **Appendix 2**).

At the introductory call the audit scope will be agreed, in consultation with the organisation; it will take into account any current known risks, generic data protection issues, as well as any organisation specific concerns there may be about its data protection policies and procedures.

The scope areas that can be covered are:

- data protection governance and accountability;
- staff data protection training and awareness;
- security of personal data;
- requests for personal data and data portability;
- direct marketing;
- 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 (**Appendix 2**).

Gathering evidence

Prior to the audit visit we will request necessary policies and procedures, pertaining 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 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 site visit.

Key personnel may be interviewed, in person or via telephone, prior to the onsite visit, to further assess the design effectiveness of controls the organisation has in place. We may also ask for operational data and KPI's used to manage SLA's or performance to gain an understanding of adherence to process.

The audit visit

The audit site visit usually takes place over two or three days. The visit will begin with an opening meeting, attended by appropriate members of the senior management 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.

We will work with the organisation to ensure that the audit visit will be productive by identifying appropriate and 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.

The methodology used by the audit team during the site visit will primarily consist of desk-side interviews with key staff. We will aim to see how processes and policies work in practice to assess their operational effectiveness. These interviews will be supplemented by visual inspections and examinations of selected processing of personal data within the organisation and, where appropriate, testing of controls. During the visit 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 in the letter of engagement. However, there are some generic areas such as the governance structure that is covered on each audit. Other examples of evidence the team might look for is in **Appendix 1**.

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 you of the finding while we are onsite and explain what actions needs 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 evidences whilst the audit team are still onsite.

Upon completion of the audit visit, 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 be issued within 10 working days of the site visit. 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 (**Appendix 3**) will then be issued and an executive summary published.

Disagreement between the two parties may occur regarding recommendations but, ultimately, it is a matter for the ICO to determine the content of the final report.

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. The final report is indicative of a 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. A final audit report is not a definitive account of an organisation's data processing activities or an endorsement of that organisation's adherence to data protection policies or compliance with data protection legislation.

Publication

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

If requested, we will include a URL link to the organisation's website to allow the public to view any related comments that the organisation may wish to make on its own website.

3. Audit follow up

A follow up audit is where an organisation shows the ICO work done towards the agreed recommendations following the original audit. It takes place between 6 to 12 months after the audit. Audits with any limited or very limited non-compliances will be asked to take part in a follow-up audit. The follow up is aligned to the findings in the original audit and will look in detail at the work done to mitigate risk and address the actions identified from the audit. Wherever possible the lead auditor of the original data protection audit will be responsible for any follow up activity undertaken

At approximately 6 to 9 months after the final audit report has been issued and published we will contact the organisation to arrange the follow up, usually by email, to request an update on the action plan. Occasionally we'll need to return in person, in which case we'll agree any on site visit requirements with the organisation as early as possible but the follow up will predominantly be conducted remotely. The follow up activities will be focused primarily on those scope areas and recommendations that were measured limited or very limited from the original assurance ratings.

We will look to ensure high priority, critical to privacy legislation recommendations have been (or are being addressed) and if not we may consider further action.

Follow up reporting

The draft follow up report will be produced in a similar way as the original audit report. We will publish an executive summary of the follow up report.

The follow up will also focus on the work done to address the limited and very limited assurance recommendations detailed in the action plan. The ICO will reserve the right to consider further action if we feel the risks identified are not being addressed.

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 visit lasts three days and dates for the production of 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 a feedback questionnaire 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, high priority recommendations, 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 article 54.2 of the GDPR not to disclose any information given under a duty of professional secrecy.

What about enforcement action?

Audits are intended to be educative and not punitive and it is not intended that audits will lead to formal enforcement action – they are seen as a way of encouraging conformance to data protection legislation as well as good practice.

However, depending on the type and severity, the Information Commissioner reserves the right to utilise its enforcement powers as a result of a serious non-compliance discovered in the course of 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.

Appendices - **Appendix 1 – Example question areas and evidence**

Governance and Accountability	Training and Awareness	Records management	Security of personal data	Subject access and data portability	Data Sharing	Information risk assessment (DPIA) and management	Direct marketing	FOI
Policies and procedures Governance structures and key roles Measures and KPI's Internal and external audits Risk register Returns DPIA's	Induction Role based training Refresher training Records and skills matrix e-learning IT access Awareness	Policies and procedures Roles and responsibilities Training and awareness Information assets Index or tracking of records Collection of data Records maintenance Retention schedules Disposal of data	Policies and Procedures Organisational structure Training and awareness Asset management Access control Physical security Operations security Communications security Supplier relationships Incident Management Business continuity Compliance	Owner/Procedures SAR log Monitoring Redaction Exemptions	Owner/authorisation Policies and procedures Training and awareness Data Privacy Impact Assessment (DPIA) Data sharing log Manging data sharing agreements Sharing protocols Disclosures Sharing agreement actual and templates Sharing agreement logs	Policies and procedures Responsibility Initiate protocols Organisational measures Consultation process Reporting Project plan/risk register Review and audit Sample DPIA's and templates Log of disclosures	Policies and procedures Consent Screening Opting in / out Fair processing notice Database management Bought-in lists Lawful basis Records management Individual rights Training and awareness Marketing methods	Governance structure Policies and procedures Monitoring Contracts Partnerships agreements Logs Consultation Complaints/Internal review Exemptions and Redactions Induction, Refresher Role based training records

Policies and procedures Intranet site Organisational charts and reporting lines Job descriptions Terms of reference Forums and meetings minutes Internal and external reports Audit reports and internal reviews	Training modules e-learning modules Central training records Refresher training material and records IT user profile requests	Policies, procedures and training records Data collection forms Fair processing notices RM systems detail RM roles and team structure Information asset register Retention schedules Destruction records and certificates	Policies and procedures IT security licences Incident logs Security standard clauses Home working risk assessments Asset registers Structures and responsibilities Key registers Audits and vulnerability testing reports	Policies and procedures Templates SAR log Training materials Performance reports Meetings minutes Copies of responses to requests Sharing protocols Roles and responsibilities	Policies and procedures Training materials Data sharing agreement logs Responses to requests Sharing protocols Roles and responsibilities Sharing agreements actual and templates	Policies and procedures Informed decision making practices Sample DPIA's and templates Log of disclosures	Policies and procedures Methods of consent Screening Opting in / out Fair processing notice Database management Bought-in lists Records management Data cleansing activity Training modules Marketing campaigns	Policies and procedures Organisational structure, roles and responsibilities FOI log Risk registers, reports Observations Job descriptions Performance data Cases/requests Minutes

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

Letter of Engagement

To: XXX.
CC: -
Date: XX/XX/XX
From: XX (Team manager (Audit))

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the General Data Protection Regulation (GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision to carry out consensual audits. Additionally Section 146 of the DPA 18 allows the ICO, through a written "assessment notice", to carry out an assessment of compliance with the data protection legislation.

1.2 The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

1.3 XXX has agreed to a consensual audit by the ICO of its processing of personal data.

2. Purpose

2.1 The primary purpose of the audit is to provide the ICO and XXX with an independent opinion of the extent to which they (within the scope of this agreed audit) are complying with data protection legislation and highlight any areas of risk to their compliance.

2.2 The audit will also review the extent to which XXX (within the scope of the audit) demonstrates good practice in their data protection governance and management of personal data.

2.3 Good data protection practice is promoted by the ICO through its website and 'The Guide to GDPR' guidance, the issue of good practice notes, codes of practice and technical guidance notes. The

ICO will use such guidance when delivering an audit opinion on 'good data protection practice'. In addition the ICO will use the experience gained from other data protection audits, appropriate sector standards and enforcement activity.

3. Scope

3.1 The audit will assess the risk of non-compliance with data protection legislation, the utilisation of ICO guidance and good practice notes and the effectiveness of data protection activities with specific reference to the agreed scope (see Appendix One).

Out of Scope

3.2 The ICO will restrict its audit activity to the departments and locations detailed and agreed within the scope and audit schedule.

3.3 The audit will not review and provide a commentary on individual cases, other than to the extent that such work may demonstrate how XXX is fulfilling its obligations and demonstrating good practice.

3.4 The ICO, however, retains the right to comment on any other weaknesses observed in the course of the audit that could compromise good data protection practice.

4. Performing the audit

4.1 The Audit Team Manager and Engagement Lead Auditor responsible for the audit will work with representatives of XXX prior to the audit:

- To gain a strategic overview of the management of personal data within the organisation and any relevant background information. This will be informed by a questionnaire sent out in advance.
- To discuss and agree the areas for pre onsite testing and schedule pre onsite interviews.
- To discuss locations for the onsite visits, the duration of onsite work required for each site and the schedule of interviews.
- To identify and agree any documented evidences such as policies and procedures that could be provided in advance of the audit onsite visit, to adequately inform the audit process.

4.2 The ICO will complete a document review and speak to key personnel prior to the onsite visit to assess the design effectiveness of controls within the scope of the audit.

4.3 The ICO will seek to visit key departments and sites within the scope of the audit and organisation as arranged with XXX. In identifying appropriate scope and locations the ICO will consider the following:

- The organisation's feedback on compliance with internal policies and procedures.
- Current and historical complaint information obtained from the ICO's case handling department.
- Common risks identified from other audits, casework and enforcement action with similar controllers.

4.4 The schedule of meetings and audit activities that is agreed will be reviewed in advance of the audit to ensure that the interviews are with an appropriate mix of managerial and operational staff and cover all of the control areas necessary to establish an assurance rating. A draft schedule and list of the controls to be covered will be provided in advance.

4.5 While on site the audit team will meet with staff to assess the operational effectiveness of controls XXX have in place to ensure they comply with their data protection responsibilities. This will be achieved through interviews with staff, reviewing relevant records, data sampling or testing and observing procedures being implemented in practice.

4.6 The ICO will require access to relevant staff 'desk side' where possible to understand how staff process personal data (limited to the scope provided).

4.7 The ICO will consider the extent to which the Internal Audit department includes data protection audits in their programmes of audit or compliance work to avoid duplication of work. Similarly, the ICO will consider any external audits that have been recently been undertaken by any accredited bodies or organisations.

4.8 The ICO will provide regular feedback on the audit progress to the nominated single point of contact at the end of each day and at the end of the audit in a closing meeting. The ICO believes that regular feedback should assist both the ICO and the organisation to quickly

understand and address emerging issues and concerns and help to avoid any misunderstanding.

4.9 During the audit the ICO will notify you of any breaches to the GDPR/DPA18 and any potential implications for follow-up or enforcement action.

4.10 The Audit Team are bound under Section 132 of the DPA 18 'Confidentiality of Information', not to disclose any information that relates to an identified or identifiable individual or business provided to them as part of the audit process.

5. Audit team

5.1 The following people will be part of the audit team. It is envisaged that x auditors will be used.

	Team Manager (Audit)
	Engagement Lead Auditor
	Lead Auditor

6. Reporting

6.1 Initially a draft report and action plan will be issued. During the drafting of the audit report input will be sought from the nominated single point of contact at XXX to ensure that the report is factually accurate. The draft report will contain details of all observations and non-conformities identified during the course of the audit. Recommendations will also be made based on the ICO's findings.

6.2 The draft action plan will be returned by XXX accepting or rejecting each of the recommendations and including a proposed action and owner for each recommendation and the date that the action will be implemented.

6.3 The draft report will provide XXX with an assurance opinion per scope area based on the work undertaken, using a framework of four categories of assurance, from high level of assurance to very limited assurance. The overall opinion(s) will be based on the existence and effectiveness of the processes, policies, procedures and practices operating to mitigate any identified risks to complying with data protection legislation.

6.4 The final report and an executive summary will be issued to agreed recipients.

6.5 The identity of organisations that are being audited is published on the ICO website as part of proactively communicating the audit

work programme. However, the ICO will not proactively publish details of the scope and findings of a consensual audit prior to the completion of the audit.

6.6 Once the audit report and executive summary have been completed and agreed the ICO will publish the executive summary on their website.

6.7 XXX will be informed in advance of the publication date.

6.8 Dependent on the findings of the final audit report, the ICO may wish to schedule a follow up – this would be discussed and agreed with XXX as appropriate.

6.9 At the start of the follow up process, XXX will provide, on request and prior to the scheduled follow up date, an update on the actions that were agreed at the conclusion of the original audit. This update should be agreed and approved by senior management prior to return.

6.10 As part of the update, XXX will be asked to provide supporting evidence to demonstrate the actions taken for the high and urgent priority recommendations from the original audit, as well as commentary on the medium and low priority actions.

6.11 If there are any concerns during the follow up review in relation to progress made by XXX towards completion of the actions agreed during the original audit, the ICO will consider whether it is appropriate to exercise her formal enforcement powers to ensure compliance with the GDPR/DPA18.

7. Timescales

	Responsibilities of the ICO	**Responsibilities of XXX**
Date the letter of engagement issued:		
Date the signed letter of engagement is returned:		
Date the list of required documents and the blank on-site schedule issued:		

Date pre audit document review evidence is returned by:		
Date the draft schedule is returned:		
Date the final schedule is returned after review against controls:		
Date of the on-site visits:		
Draft report and action plan issued	Within 10 working days of the onsite visit	
Action plan returned		Within 10 working days of receipt of the draft report and action plan
Final report and executive summary issued	Within 5 working days of receipt of the completed action plan	

The ICO commits substantial planning and resources into arranging the audit. Postponements and deviations from agreed timescales above have the potential to impact detrimentally on our audit programme and the service we offer. Your co-operation in meeting the deadlines is very much appreciated.

8. Contacts

8.1 Key Contact at XXX: XXX

Key Contact at ICO: XXX – Engagement Lead Auditor

9. Logistics

9.1 Individual onsite arrangements for access and audit and any pre onsite visit phone calls will be organised through XXX at XXX.

9.2 Where possible interviews will be carried out 'desk side'. With the exception of reviews and interviews undertaken at specialist technical sites which may be conducted at a pre agreed location.

9.3 Rooms will be made available, where possible, to the Information Commissioner's auditors at sites identified in the schedule to carry out interviews when it is not appropriate to work 'desk side'. No remote network access is required by ICO auditors.

10. Expected Added Value

10.1 XXX will receive an independent opinion in relation to their compliance with data protection legislation and progress towards the implementation of good practice within the scope of the audit.

10.2 XXX staff will have the opportunity to discuss and exchange actual data protection issues and examples of good practice with the members of the Information Commissioner's audit team.

10.3 XXX will be assured of a proportionate consideration of the risk and impact of non-compliance through the data protection knowledge and experience of the auditors.

10.4 The ICO will gain an improved understanding of XXX, its structure and data protection governance and the sector that it operates in to help inform its decision making and approach to guidance.

Client Comments

I agree to the scope of the audit as set out in this Letter of Engagement and to ensure that adequate resource is provided to allow the audit to be prepared for and carried out satisfactorily.

Agreed by Client

Signed:

Position:

Date:

Appendix 3 - Example audit report

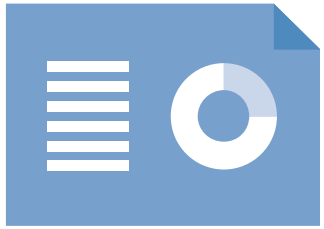
Any Public Authority Anywhere

Data protection audit report

Month 201X

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the General Data Protection Regulations (GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision 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.

[Detail of circumstances that led to the audit (post May 2018 this may include whether the audit is consensual).]

The purpose of the audit is to provide the Information Commissioner and <name> with an independent assurance of the extent to which <name>, 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**

The audit was 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, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist data controller 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. Data controller's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

****Signpost appendices, where necessary****

Audit Summary

INSERT TABLE FROM 'GRAPHS and CHARTS' TAB

Priority Recommendations

INSERT CHART FROM 'GRAPHS and CHARTS' TAB

Graphs and Charts

INSERT RELEVANT CHARTS AND GRAPHS FROM 'GRAPHS and CHARTS' TABS.

Areas for Improvement

Insert short summary of key themes that have been identified during the audit where opportunities for improvement have been acknowledged (could be based on Closing Meeting feedback).

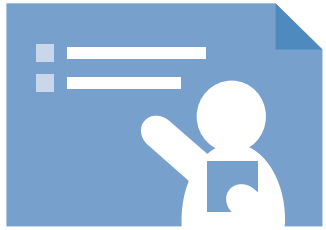
Good Practice (*optional)

Where applicable, insert short summary of any good practice (above control measure benchmark) that has been identified during the audit. If no good practice identified, delete section title.

THIS PAGE IS INTENTIONALLY LEFT BLANK TO ALLOW TEXT TO CARRY ACROSS FROM THE PREVIOUS PAGE.

IF THIS PAGE IS NOT REQUIRED IT SHOULD BE DELETED.

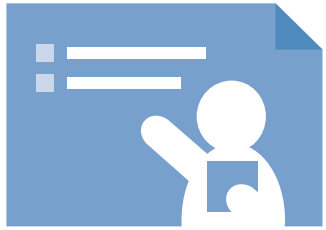
Audit findings



The table/tables below identifies/identify areas for improvement that were identified in the course of our audit; it/they include/includes recommendations in relation to how those improvements might be achieved.

INSERT TABLE

Appendices

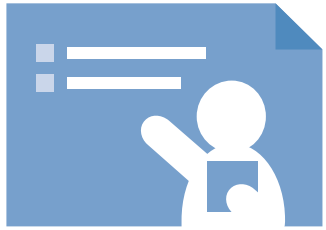


Appendix One – Recommendation Priority Ratings Descriptions

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.

OTHER APENDICES eg INSERT PHOTOS with captions to highlight relevant findings or INSERT SURVEY INFO

Credits



ICO Audit Team

ICO Team Manager - name
ICO Engagement Lead Auditor – name
ICO Lead Auditor - name

Thanks

The ICO would like to thank name and job title of contact for their help in the audit engagement.

Distribution List

This report is for the attention of names and job titles (to incl. point of contact and individual who signed LoE as a minimum).

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 data controller.

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