Auditing data protection

a guide to ICO data protection audits

ico.
Information Commissioner's Office

Contents

	Executive summary	3
1.	**Audit programme development** Audit planning and risk assessment	5
2.	**Audit approach** Gathering evidence Audit visit Draft and final reports Publication	6
3.	**Audit follow up and reporting** Audit follow up Follow up reporting	9
4.	**Frequently asked questions**	10
5.	**Appendices** 1. Scope areas 2. Example letter of engagement 3. Example audit report 4. Example follow up report	13

Executive summary

The Information Commissioner, who is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA), 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 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.

Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. Good practice is defined in the DPA as practices for processing personal data which appear to be desirable. This includes, but is not limited to, compliance with the requirements of the DPA. This is known as a consensual audit.

The benefits of a consensual audit include:

- helping to raise awareness of data protection;
- showing an organisation's commitment to, and recognition of, the importance of data protection;
- the opportunity to use the 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; and
- the sharing of knowledge with trained, experienced, qualified staff and an improved working relationship with the ICO.

The focus of the audit is to determine whether the organisation has implemented policies and procedures to regulate the processing of personal data and that processing is carried out in accordance with such policies and procedures. When an organisation complies with its requirements, it is effectively identifying and controlling risks to prevent breaching the DPA.

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

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

The scope will be agreed prior to the audit and in consultation with the organisation. It will take into account both generic data protection issues as well as any organisation specific concerns about data protection policies and procedures. It will also identify relevant data protection risks within organisations.

The ICO proactively publishes its audit programme on the ICO website and as such the identity of organisations that agree to an audit are published. This only has basic details and does not include the agreed scope of the audit.

The ICO will make recommendations on how to mitigate the risks of non compliance, reducing the chance of damage and distress to individuals and regulatory action being taken against the organisation for a breach of the DPA.

Following completion of the audit, we will provide a comprehensive report along with an executive summary. The audit report provides an opportunity to respond to observations and recommendations made by the audit team. The executive summary is published on the ICO website with agreement from the organisation. Examples of executive summaries can be seen on the 'evaluating good practice' pages of the ICO website.

The ICO also has the power to conduct compulsory audits, under section 41a of the DPA. This enables the Information Commissioner to serve government departments, designated public authorities and other categories of designated persons with a compulsory 'assessment notice' to evaluate their compliance with the data protection principles. The assessment notices code of practice provides further guidance on compulsory audits.

1. Audit programme development

Audit planning and risk assessment

In line with the Regulators' Compliance Code, the Information Commissioner has adopted a risk-based, proportionate and targeted approach to audit activities. This approach takes account of the Chartered Institute of Internal Auditors standards of risk-based auditing. This allows ICO auditors to focus on organisations striving to comply with the DPA, but where there is a risk of failure. To identify high-risk data controllers and sectors the ICO uses a number of sources, including:

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

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

Audit planning risk assessment, in line with the Hampton Review recommendations and the Regulators' Compliance Code, will be based on:

- the potential impact of non compliance; and
- the likelihood of non compliance.

In determining the risks of non compliance one or more of the following factors will be considered:

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

- internal or external audits conducted on data controllers related to data protection and the processing of personal data;
- notification details 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 privacy impact assessments carried out by the data controller.

In determining the impact 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 strategic liaison; and
- those identified by enforcement investigation.

These organisations are also considered on a risk basis taking into account the factors outlined above.

2. Audit approach

Once an organisation has consented to an audit, an introductory meeting will be arranged to discuss the audit process and the ICO audit programme will be updated on the ICO website. A provisional time for the audit site visit will also be agreed by working with organisations to fit with their other commitments and to minimise the impact on their day to day work. A draft letter of engagement will be used as an agenda at the initial meeting to develop the scope of the audit and set appropriate timescales (see **Appendix 2**).

The scope will be agreed in consultation with the organisation. It will take into account both generic data protection issues as well as any organisation specific concerns there may be about its data protection policies and procedures. It will also identify relevant data protection risks within the organisation.

Examples of common scope areas are:

- data protection governance;
- staff data protection training and awareness;
- security of personal data (manual and/or electronic);
- requests for personal data;
- information sharing;
- records management; and
- Privacy Impact Assessments.

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

Within two days of the meeting we will issue a formal letter of engagement (**Appendix 2**).

Gathering evidence

Prior to the audit visit we will request as necessary policies and procedures that cover the 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 will be used to inform the direction of the audit visit and are reviewed at the ICO's offices prior to the site visit.

We will work with the organisation to ensure that the audit visit will be productive by identifying appropriate key stakeholders to interview and relevant processes to examine. These interviews will be agreed in a schedule, drawn up by the organisation in consultation with the audit team.

The audit visit

The audit site visit usually takes between two and three days. At the start of the visit, we will arrange for an opening meeting with appropriate members of the senior management of the organisation to explain the process to them. This provides an opportunity to discuss any issues and answer any questions about the process.

The methodology used by the audit team during the actual visit is primarily a question/interview based approach. This is supplemented by visual inspections and examinations of selected uses of personal data within the organisation. During the visit all auditors will make notes 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 which are normally covered within each scope area, and examples of these and the evidence that the audit team might look for, is within **Appendix 1**.

The most important element of an audit from the perspective of the audit team is that access to key systems and data is provided by the auditee and that questions posed by the audit team are answered comprehensively and accurately.

Upon completion of the audit visit, the audit team will hold a 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 will also be given.

Draft and final reports

As detailed in the letter of engagement, the first draft report will be issued within 10 working days of the site visit. The report will define and grade risks, detail findings and issues identified against those risks and provide an overall audit opinion. The overall audit opinion is provided following a review of each individual scope area assessed during the visit.

The organisation will be required to check the first draft for factual accuracy and return their approval and/or any amendments to the audit team.

Following return of the first draft by the organisation, the second draft report will encompass these amendments and also include recommendations. The recommendations made will mitigate the risks of non compliance, reducing the chance of damage and distress to individuals and/or the chance of regulatory action being taken against the organisation for a breach of the DPA. The ICO will complete and deliver the second draft within the timescales detailed in the letter of engagement.

The report will then be issued to the organisation with a draft executive summary. The executive summary will be a template of high level sections taken from the report and produced in a different format for publication. The organisation will be given 10 working days to agree the summary.

The organisation will be required to agree 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 with a request for authority to publish the executive summary.

All factual inaccuracies will be amended by the audit team. Disagreement between the two parties may occur regarding recommendations. 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. A positive final report is indicative of a level of assurance regarding an organisation's policies and procedures in respect of the DPA at a certain point in time, in relation to the agreed scope areas. The final draft of an audit report agreed by both parties is not a definitive account of an organisation's data processing activities or an endorsement of that organisation's adherence to data protection policies.

Publication

The audit programme is published in advance. After an audit we will ask the organisation to agree to us publishing the executive summary on the ICO website. If it agrees, we will publish. If it does not agree, we will publish a comment on our website that an audit took place but that the organisation declined to have the executive summary published.

If requested, we will include a URL link to the organisation's website to allow the public to view any related comments the organisation makes on its own website. The table below shows how the published details appear on the web site.

[Date]
The ICO has carried out a data protection audit of [name of org] with its consent.

Read the executive summary of the audit report [link]

Read more about the audit on the [name of org] website [link]

[Date]
The ICO has carried out a data protection audit of [name of org] with its consent. [Name of org] has asked us not to publish the executive summary of the audit report.

Read more about the audit on the [name of org] website [link]

The ICO will not proactively publicise details of consensual audit reports. However, there may be instances in which publicising a report would help to educate other data controllers, prevent further breaches, or be of

interest to the public. In these cases we would look for consent from the organisation concerned.

More information regarding publishing and publicising audits is available in our communicating audits policy.

3. Audit follow up

Wherever possible the lead auditor of the original data protection audit will be responsible for any follow up activity undertaken. A review of the initial audit will be undertaken, considering the actions required and taking into account the previous audit opinion.

Generally the likelihood of follow up action will conform to the rules below, taking into account individual completion dates of required action.

Audits initially rated green - no follow up.

Audits rated yellow – the organisation will send us an email update at six months and we may comment upon progress.

Audits rated amber – we will conduct an email follow up at six months and we will produce a short follow up report.

Audits rated red – we will require three monthly updates from the organisation and a full update from them at 12 months. A follow up site visit will be required covering the same scope areas. A full follow up report will be produced.

We will contact the organisation, usually by email, to request an update on actions taken to address the recommendations. We will agree any on site visit schedule with the organisation and the process will be the same as above for an audit.

Follow up reporting

The draft follow up report (appendix 4) for red, 'very limited assurance' reports, will be produced in the same way as the original audit report. Similar to the process of publishing the original report, we will seek permission to publish an executive summary of the follow up report.

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 draft 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.

What about freedom of information requests?

The ICO may receive requests under the Freedom of Information Act 2000 to disclose specific audit reports. All requests for information are looked at on a case by case basis. We would always consult with the organisation in question before responding to a request for information.

In the past, we have received and responded to a number of information requests for specific audit reports. We have dealt with requests where we have withheld a report in its entirety, provided a redacted report and provided a report in full.

The basis for this approach is in section 59 of the DPA which relates to information provided to the Information Commissioner and his staff. This states that ICO staff shall not disclose information:

a. which has been obtained by or given to them under the DPA;
b. relates to an identifiable individual or business; and
c. is not at the time of disclosure, and has not previously been, available to the public from other sources

unless the disclosure is made lawfully.

In most cases where the information being requested is an audit report, for the disclosure to be lawful, we would have to have the consent of a representative of the organisation concerned.

Can you publish without our consent?

For consensual audits, we will not publish the executive summary without permission. This is a high level document and contains only the background to the audit, the overall audit opinion and the areas of good practice/needing improvement. The detailed findings contained in the back of the report are not published.

We do though proactively publish a list of organisations who have agreed to audit in the form of an ICO audit programme.

What about confidentiality?

Any member of the ICO is legally bound, under section 59 of the DPA, not to disclose any information given to it for the purposes of the DPA. Paragraph three of that section stipulates that if we were to do so it would be a criminal offence and we would be liable to prosecution.

What about enforcement action?

Audits are supposed 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 compliance and good practice. However, we do reserve the right to use our enforcement powers in case of any identified major non compliance where the data controller refuses to address a recommendation within an acceptable timescale.

The Information Commissioner will not impose a monetary penalty as a result of a non compliance discovered in the course of an audit.

Are the team qualified?

The ICO audit team are all IIA (Institute of Internal Auditors) qualified and hold the ISEB (Information Systems Examination Board) certificate in data protection (or are working towards those qualifications), as well as having a range of skills and backgrounds including data protection casework, 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**

Data protection Governance	Training and Awareness	Records management	Security of personal data	Requests for personal data	Data Sharing	Privacy Impact Assessments	FOI requests
Policies and procedures Governance structures Measures Audits Risk register Returns Privacy impact assessment	Induction Role based training Refresher Records e-learning IT access Awareness	Roles and responsibilities Policies and procedures Training and awareness Information assets Index and tracking of records Collection of data Maintenance of records Retention schedules Disposal of data	Policy Organisation Training and awareness Asset management Access control Physical security Operations security Communications security Supplier relationships Incident management Business continuity management Compliance	Owner/procedures SAR Log Monitoring Redaction Exemptions	Owner/authorisation Policies and procedures Training and awareness Privacy impact assessment Data sharing log Managing data sharing arrangements Sharing protocols Disclosures	Policy Responsibility Organisational measures Consultation process Reporting Project Plan/Risk register Review and audit	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 Organisation charts Job descriptions Terms of reference Minutes of meetings Internal and external reports Audit reports	Training presentation e-learning module Central training records Refresh training material and records IT user profile requests	Policies procedures and training records Data collection forms Fair processing notices Records management systems detail RM roles and team structure Information asset register Retention schedules Destruction records and certificates	Policies and procedures IT security licenses Incident logs Security standard clauses Home working risk assessment Asset registers Structures and responsibilities Key registers Audits and vulnerability testing reports	Policies and procedures Templates SAR log Training materials Performance reports Minutes of meetings Copies of responses to requests System review	Policies and procedures Training materials Data sharing agreement logs Responses to requests Sharing protocols Roles and responsibilities	Introduction of new policies, systems or revised ISA Job descriptions, organisational charts, project management responsibilities Examples of screening or staged sign off of projects. Documented consultation and results Example PIA and audit reports, risk registers	Policy and procedures Organisational structure, roles and responsibilities FOI log Risk registers, reports Observations Job descriptions Performance data Cases/requests Minutes

Appendix 2 – Letter of Engagement

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: Named contact.
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 the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 [If appropriate add detail of circumstances that led to the audit – undertakings, self reported breaches, risk assessment leading to letter to insurance companies/council/NHS etc.]

1.4 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 the DPA 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 Where appropriate and with the agreement of both parties, the audit may also assess compliance with obligations under both the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

2.4 Good data protection practice is promoted by the ICO through its website and 'The Guide to Data Protection' document, 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 scope is limited to the XXX departments/sections of XXX and will assess the risk of non compliance with appropriate data protection principles, the utilisation of ICO guidance and good practice notes and the effectiveness of data protection activities with specific reference to:

[Audits will cover a maximum of 3 scope items]

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

c. 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.

d. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

e. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

f. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

g. Privacy Impact Assessments - An effective PIA will be used throughout the development and implementation of a project, using existing project management processes. A PIA enables an organisation to systematically and

thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

As per section 2.3 above, the following scope area may also be included in the audit (see also the associated risk in section 4):

h. Freedom of Information - The processes in place to respond to any requests for information and the extent to which FOI/EIR responsibility, policies and procedures, training, performance controls, and compliance reporting mechanisms are in place and in operation throughout the organisation.

Out of Scope

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

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

3.4 The audit will not review XXXXXX.

3.5 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. Risks

The ICO has identified broad risk areas applicable to the agreed audit scope. The ICO believes that the absence of appropriate arrangements in these areas threatens the organisation's ability to meet its data protection obligations.

a. Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the DPA resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

b. If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the DPA resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

c. In the absence of appropriate records management processes, there is a risk that records may not be processed in compliance with the DPA resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

d. Without robust controls to ensure that personal data records are held securely in compliance with the DPA, there is a risk that they may be lost or used inappropriately, resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

e. Without appropriate procedures there is a risk that personal data is not processed in accordance with the rights of the individual and in breach of the sixth principle of the DPA. This may result in damage and/or distress for the individual, and reputational damage for the organisation as a consequence of this and any regulatory action.

f. The failure to design and operate appropriate data sharing controls is likely to contravene the principles of the DPA, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.

g. Without effective processes in place to facilitate "privacy by design", there is the risk that the privacy implications of projects and resulting potential areas of non-compliance with the Data Protection Act 1998 will not be identified at an early stage. This may result in regulatory action, reputational damage to the organisation and damage or distress to the individuals who are the subject of the data.

h. Without a process for responding to requests for information, supported by an appropriate governance framework and training regime for ensuring the effectiveness of FOI/EIR procedures, there is a risk that information will not be made available in compliance with the FOIA/EIR, resulting in regulatory action, dissatisfaction by individuals and/or reputational damage.

5. Performing the audit

5.1 The Audit Team Manager responsible for the audit will meet 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 appropriately refine and agree the 3 scope areas for the audit.
- To discuss locations for the visits and the duration of on site work required for each site.
- To identify and agree any policies and procedures that could be provided in advance of the audit site visits, to adequately inform the audit process.

5.2 The ICO will seek to visit key departments and sites within the scope of the audit and organisation as arranged with XXX.

5.3 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 data controllers.

5.4 A schedule of meetings and audit activities will be agreed with the nominated single point of contact for the audit and the identified business areas. This will be reviewed in a meeting/call 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.

5.5 While on site the audit team will meet with staff to establish if controls are in place to ensure the organisation complies with its data protection responsibilities. This will be achieved through interviews with staff, reviewing relevant records and observing procedures being implemented in practice.

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

5.7 Space will be usually be allocated in the schedule of interviews for testing and evidence gathering.

5.8 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.

5.9 As far as is practicable and appropriate the ICO will provide regular feedback on audit progress to the nominated single point of contact at the end of the first and second 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.

6. Audit team

6.1 The following people will be part of the audit team. It is envisaged that 2 auditors will be used.

XXX	Team Manager (Audit)
XXX	Engagement Lead Auditor
XXX	Lead Auditor/Auditor

7. Reporting

7.1 Initially a first draft report will be issued detailing the audit findings but without the assurance ratings and recommendations. Input will be sought from the nominated single point of contact to ensure that the report is factually accurate.

7.2 Following any amendments for accuracy a second draft report will be issued complete with any appropriate recommendations. This draft will be returned by XXX accepting or rejecting each of the recommendations and including an action plan that shows an owner for each recommendation and the date that the action will be implemented.

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

7.4 The report will provide XXX with an overall assurance opinion 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 will be based on the effectiveness of the processes, policies, procedures and practices operating to mitigate any identified risks to complying with the DPA.

7.5 Each of the scope areas/risks identified in sections 3 and 4 will be similarly categorised. The rating will take into account the impact of the risk and the probability that the risk will occur.

7.6 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. The ICO has an operating memorandum of understanding (MOU) with the Care Quality Commission (CQC). In the case of NHS audits, the ICO will share audit scheduling information with the CQC prior to audits. Where, during the course of conducting an audit the ICO identifies any significant failings which may significantly impact upon patient care, it may also share these with the CQC. This will help ensure regulatory resources are targeted appropriately and that work is not duplicated.

7.7 Once the audit report and executive summary have been completed and agreed the ICO will publish a statement on its website to indicate that a data protection audit has been completed and will seek agreement from the organisation to publish the executive summary with a 10 working day deadline for response.

7.8 If XXX do not respond within the 10 working day timeframe it will be perceived as consent being withheld and the ICO website will be updated to say that the audit took place but permission to publish the executive summary was withheld.

7.9 XXX will be informed in advance of the publication date and will be provided with the opportunity to provide a link to its own website for any further organisational comments it wishes make.

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

7.11 The type of follow up activity undertaken will be determined by the overall assurance provided by the initial audit. A follow up report will not be produced where the original assurance level is either high or reasonable. Where the initial assurance is reasonable, the ICO will request a progress update signed off at Board level within XXX. We will review this and reserve the right to comment on priority recommendations which we feel have not been adequately addressed within the update.

7.12 Follow up of reports that are limited assurance will be based solely on a progress update signed off at Board level. We will produce a short report summarising progress against the recommendations although this will not include a revised assurance rating. We will however express any serious concerns we have regarding lack of progress against the recommendations.

7.13 Where the initial assurance is very limited, the ICO and XXX commit to conduct a follow up audit of the same scope areas as the original. Following this, the ICO will produce a second audit report including a new assurance rating. No further action or follow up will take place after this and mitigation of the risks identified will be the sole responsibility of XXX.

7.14 Where appropriate, the ICO will also produce a follow up executive summary which it will agree with XXX.

7.15 Once the follow up report and follow up executive summary have been completed and agreed, the ICO will publish a statement on its website to indicate that a follow up has been completed and will seek agreement from the organisation to publish the follow up executive summary with a 10 working day deadline for response.

7.16 If XXX do not respond within the 10 working day timeframe it will be perceived as consent being withheld and the ICO website will be updated to say that the follow up took place but permission to publish the executive summary was withheld.

7.17 XXX will be informed in advance of the publication date and will be provided with the opportunity to provide a link to its own website for any further organisational comments it wishes make.

8. Timescales

	Responsibilities of the ICO	**Responsibilities of XXX**
Date the letter of engagement and the list of required documents issued:	Within two working days from date of initial meeting. XX/XX/XX	

Date the signed letter of engagement is returned:		Within 10 working days of receipt of the LoE. XX/XX/XX
Date the blank schedule is issued for completion:	Six weeks before the audit. XX/XX/XX	
Date the policy documents and draft schedule are returned:		One month before the audit. XX/XX/XX
Date the final schedule is returned after review against controls:		Two weeks before the audit. XX/XX/XX
Date of the on-site visits:	XX – XX XXX 201X.	
Date on which the first draft report is issued:	Within 10 working days from auditors return to office. XX/XX/XX	
Date on which the comments on the first draft are provided:		Within 10 working days from receipt. XX/XX/XX
Date on which the second draft and draft executive summary is issued:	Within 5 working days from receipt of first draft with comments. XX/XX/XX	
Date on which the second draft showing the action plan is returned:		Within 10 working days from receipt of updated first draft. XX/XX/XX
Date on which the final report and executive summary is issued:	5 working days from receipt of second draft with action plan. XX/XX/XX	
Date on which the decision on whether or not to publish the executive summary is provided:		Within 10 working days from receipt of the executive summary and final report version. XX/XX/XX

The ICO commits subst rces into arranging the audit. Postpone meeting the deadlines is very much appreciated.

9. Contacts

9.1 Key Contact at XXX: XXX

Key Contact at ICO: XXX – Lead Auditor

10. Administration

10.1 Individual site arrangements for access and audit will be organised through XXX at XXX.

10.2 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.

10.3 A room 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' while they are not conducting interviews / examinations. No remote network access is required.

11. Confidentiality and security clearance

11.1 All ICO staff including the Audit Team are legally bound by Section 59 of the DPA which creates a specific criminal offence for them to knowingly and recklessly disclose any information given to the ICO for the purposes of the fulfilling it's functions (which includes audit). ICO staff are made aware of the obligation on them and the potential consequences.

11.2 All auditors are security cleared to SC level through the Ministry of Justice.

12. Expected Added Value

12.1 The ICO audit team all have, or are working towards, an Institute of Internal Auditors qualification as well as the Information Systems Examination Board certificate in data protection, as well as having a range of skills and backgrounds.

12.2 The provision of an independent opinion in relation to compliance with the DPA and progress towards the implementation of good practice.

12.3 The opportunities for staff to discuss and exchange actual data protection issues and examples of good practice with the members of the Information Commissioner's audit team.

12.4 The data protection knowledge and experience of the auditors enables a proportionate consideration of the risk and impact of non-compliance to be taken.

12.5 An improved understanding by the ICO of XXX, its structure and data protection governance and the sector that it operates in to help inform it's decision making and approach to guidance.

Client Comments

I agree the scope of the audit as set out in this Letter of Engagement.

Agreed by Client

Signed:
Position:
Date:

Appendix 3 - Example audit report

Organisation name

Data protection audit report

Information Commissioner's Office

Auditors: XXXX

Data controller contacts:

Distribution:

Date of first draft: XXXX

Date of second draft: XXXX

Date of final draft: XXXX

Date issued: **XXXX**

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.

Contents

1. Background page XX
2. Scope of the audit page XX
3. Audit opinion page XX
4. Summary of audit findings page XX
5. Audit approach page XX
6. Audit grading page XX
7. Detailed findings and action plan page XX
8. Appendix A page XX

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 [Detail of circumstances that led to the audit.]

1.4 <name> has agreed to a consensual audit by the ICO of its processing of personal data.

1.5 An introductory meeting was held on <date> with representatives of <name> to identify and discuss the scope of the audit and after that on <date> to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with <Name>, it was agreed that the audit would focus on the following areas:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

c. Records management (manual and electronic) – The processes in place for managing both manual and electronic records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

d. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

e. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

f. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

g. Privacy Impact Assessments - An effective PIA will be used throughout the development and implementation of a project, using existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

h. Freedom of Information - The processes in place to respond to any requests for information and the extent to which FOI/EIR responsibility, policies and procedures, training, performance controls, and compliance reporting mechanisms are in place and in operation throughout the organisation.

3. Audit opinion

3.1 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 the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion – to be included in second draft	
Very limited assurance	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. Comments specific to audit We have made XXXX very limited/limited/reasonable/high, XXXX very limited/limited/reasonable/high and XXXX very limited/limited/reasonable/high assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report, along with management responses.
Limited assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.

	Comments specific to audit We have made XXXX very limited/limited/reasonable/high, XXXX very limited/limited/reasonable/high and XXXX very limited/limited/reasonable/high assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report, along with management responses.
Reasonable assurance	There is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA. Comments specific to audit We have made XXXX very limited/limited/reasonable/high, XXXX very limited/limited/reasonable/high and XXXX very limited/limited/reasonable/high assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report, along with management responses.
High assurance	There is a high level of assurance that processes and procedures are in place and 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 the DPA. Comments specific to audit We have made XXXX very limited/limited/reasonable/high, XXXX very limited/limited/reasonable/high and XXXX very limited/limited/reasonable/high assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7

	of this report, along with management responses.

4. Summary of audit findings

4.1 Areas of good practice

4.2 Areas for improvement

5. Audit approach

5.1 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.

5.2 The audit field work was undertaken at <location/s> between <dates>.

6. Audit grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Recommendation priority	Definitions
	High assurance	Minor points only are likely to be raised	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 the DPA.
	Reasonable assurance	Low priority	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 the DPA.
	Limited assurance	Medium priority	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 the DPA.
	Very limited assurance	High priority	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.

7. Detailed findings and action plan

7.1 Scope A: Data Protection Governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

Risk: Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the Data Protection Act 1998 resulting in regulatory action and/or reputational damage.

a1. Finding. **********.

a2. Finding. **********.

a3. Finding where there was good practice. **********

a4. Finding. **********

a5. Finding where there was an uncontrolled or poorly controlled risk that will require a recommendation to improve practices.

Recommendation: *.**

Management response: Accepted/Partially Accepted/Rejected.
Owner. Date for implementation.

a6. Finding. Finding where there was good practice. **********.

a7. Finding. **********

a8. Finding where there was an uncontrolled or poorly controlled risk that will require a recommendation to improve practices.

Recommendation: *.**

Management response: Accepted/Partially Accepted/Rejected.
Owner. Date for implementation.

7.X The agreed actions will be subject to a follow up audit to establish whether they have been implemented.

7.X Any queries regarding this report should be directed to <name>, Engagement lead auditor, ICO Audit.

7.X During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

Appendix A

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 3 months	Progress at 6 months
Include all recommendations reflecting the numbering in the report	Taken from final version	Describe the status and action taken.	Describe the status and action taken.

Appendix 4 – Example follow up visit report

Organisation name

Follow-up data protection audit report

Information Commissioner's Office

Auditors: XXXX

Data controller contacts:

Distribution:

Date of first draft: XXXX

Date of second draft: XXXX

Date of final draft: XXXX

Date issued: **XXXX**

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.

Contents

1. Background (follow-up assessment) page 04
2. Follow-up audit conclusion page XX
3. Summary of follow-up audit findings page XX

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 The original audit took place at <name> premises on [insert date] and covered [insert scope areas]. The ICO's overall opinion was that there was [High/Reasonable/Limited/Very Limited] assurance that processes and procedures are in place and being adhered to. The ICO identified some scope for improvement in existing arrangements in order to achieve the objective of compliance with the DPA.

1.4 XXX recommendations were made in the original audit report. <name> responded to these recommendations [positively, agreeing to formally document procedures and implement further compliance measures].

1.5 The objective of a follow-up audit assessment is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks and thereby support compliance with data protection legislation and implement good practice.

1.6 A desk based follow-up took place in [insert date] to provide the ICO with a measure of the extent to which <name> had implemented the agreed recommendations This was based on management updates from <name> signed off at Board Level

2. Follow-up audit conclusion

Scope area	Number of recommendations in each scope area from the original audit report	Number of actions complete, partially complete and not implemented.
Data Governance	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Training & Awareness	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Records Management	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Security of data	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Subject Access Requests	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Data Sharing	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Privacy Impact Assessments	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented
Freedom of Information requests	XXXX	XXXX Complete XXXX Partially complete XXXX Not implemented

Section 3 below summarises the main findings of this review and highlights any residual high risk areas.

3. Summary of follow-up audit findings

3.1 A summary of the key points to include main improvements and the main high risk areas still outstanding.

3.2 xxx

3.3 xxx

3.4 Any queries regarding this report should be directed to, XXX Lead Auditor.

3.5 Thanks are given to XXX who was / were instrumental in providing the information to complete the follow-up audit.