

Auditing data protection: a guide to ICO data protection audits

Contents

Executive summary	2
1. Audit programme development Audit planning & risk assessment	4
2. Audit approach Gathering evidence Audit visit Draft and final reports Publication	5
3. Audit follow up and reporting Audit follow up Follow up reporting	9
4. Frequently asked questions	9
5. Appendices Scope areas Example letter of engagement Example audit report Example follow up report	12

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 Act as practices for processing personal data which appear to be desirable. This includes, but is not limited to, compliance with the requirement of the Act. 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 Act.

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 these policies and procedures are being followed;
- test the adequacy of controls in place;
- identify any potential or real 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 may 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 breach of 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 'conducting audits' 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 data protection principles. The [Assessment notices code of practice](#) provides further guidance on compulsory audits.

1. Audit programme development

Audit planning & 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 the 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:

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

- statement of internal control and / or other information published by the data controller which highlights issues in the processing of personal data;
- internal / 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, 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 discussion will be arranged to discuss the audit process. A provisional time for the audit site visit will also be agreed at this stage by working with organisations to fit with other commitments and to minimise the impact on day to day work. A draft letter of engagement which will be used as an agenda at the initial meeting to develop scope and 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 your data protection policies and

procedures. It will also identify relevant data protection risks within the organisation being audited.

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
- records management

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.

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 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, in consultation with the audit team, by the organisation before the start of the audit.

The audit visit

The audit visit usually takes between two to three days. At the start of the site visit, we will arrange 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 regarding 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 on-site 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 12 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 provided with the opportunity 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 breach of DPA. The ICO will complete and deliver the second draft within the timescales detailed in the letter of engagement.

The organisation will be asked 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 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 provided with five working days to agree the 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 and 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

Agreement to publish the executive summary on our website will be requested from the organisation. If agreement is given the executive summary will be published on the ICO website – if not agreed, a comment will be published on the website that an audit took place but the organisation declined to have the executive summary published. A URL link to the organisation's website will be included to allow the public to view any comments by the organisation on their website if requested.

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 follow up audit will be conducted by members from the original data protection audit team. They will firstly undertake a review of the initial audit, considering the actions required and taking into account the outcome of the original audit.

A risk based approach is taken to follow up activity, which will normally be informed by the assurance level given in the original audit report. An audit opinion which indicated a lower level of assurance may be followed up by a site visit to check on progress against agreed actions whereas reports with a higher level of assurance may be followed up by obtaining email and phone updates from the organisation on progress.

The timing of the follow up will normally take account of the action plan completion dates agreed by management in the original audit report. If an audit site visit is required, the timing and schedule will be agreed with the organisation in advance.

Follow up reporting

The draft follow up report (**Appendix 4**) will be produced within six days of completing the follow up visit. 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, redacted a 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 Act;
- 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.

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

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.

What about confidentiality?

Any member of the Information Commissioner's Office is legally bound, under section 59 of the Data Protection Act 1998, not to disclose any information given to it for the purposes of the Act. 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 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 all have, or are working towards, an IIA (Institute of Internal Auditors) qualification as well as the ISEB (Information Systems Examination Board) certificate in data protection, 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 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
<p>Policies and procedures Governance structures</p> <p>Measures Audits Risk register</p> <p>Returns Privacy impact assessment</p>	<p>Induction Role based training</p> <p>Refresher Records e-learning</p> <p>IT access Awareness of where to find out about data protection & ease of access to it.</p>	<p>Roles and responsibilities Policies and procedures</p> <p>Training and awareness Information assets Indexing and Tracking of records</p> <p>Collection of data Maintenance of records</p> <p>Retention schedules</p> <p>Disposal of data</p>	<p>Owner/responsibility Physical security - manual records</p> <p>Network security Mobile media Home working</p> <p>Staff monitoring Third party contracts</p> <p>Incidents</p>	<p>Owner/procedures Log</p> <p>Monitoring Redaction Exemptions</p> <p>Disclosures Sharing protocols</p> <p>Managing data sharing arrangements</p>
Example evidence				
<p>Policies and procedures Intranet site Organisation charts Job descriptions Terms of reference Minutes of meetings Internal reports External reports Audit Reports Risk registers PIAs</p>	<p>Training presentation e-learning module Central training records Refresher training records IT profile requests</p>	<p>Policies and procedures Data collection forms Fair processing notices Records management systems detail RM roles and team structure Training records Information asset register Retention schedules Destruction records and/or certificates 3rd party contracts for storage and/or destruction</p>	<p>Policies and procedures Key registers IT security licenses Incident log Security standards clauses Home working risk assessments register of mobile media Security standards clauses</p>	<p>Policies and procedures SAR log Sharing protocols Performance reports</p>

Appendix 2 – Example letter of engagement

Letter of engagement

ICO, XXXX audit

To: XXXX
CC:
Date: XX/XX/XX
From: XXXX

1. Background

- 1.1 The Information Commissioner may, with the consent of the data controller, assess the extent to which good practice is applied when processing personal data and shall inform the data controller of the results of the assessment. (Data Protection Act (DPA) 1998 s51, (7))
- 1.2 The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach. (Assessment notices code of practice 2.1)
- 1.3 An Assessment notice is the medium through which the Information Commissioner's Office (ICO) will seek to instigate a compulsory audit. However, the Assessment notices code of practice, in the interests of clarity, distinguishes between compulsory and consensual audits. (Assessment notices code of practice, 2.1, Para 6 & Appendix A.)

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual data protection audits.

- 1.4 This paragraph specific to the circumstances
- 1.5 XXXX 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 Information Commissioner and XXXX with an independent opinion of the extent to

which XXXX, within the scope of this agreed audit is complying with the Data Protection Act (DPA).

- 2.2 The audit will further seek to establish the extent to which XXXX (within the scope of the audit) demonstrates 'good practice' in its 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 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 and ICO Enforcement team work.

3. Scope

- 3.1 The audit scope will assess 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:
 - a. XXXX
 - b. XXXX
 - c. XXXX
 - d. XXXX
 - e. XXXX

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 XXXX is fulfilling its obligations and demonstrating good practice.
- 3.4 The audit will not review insert appropriate

- 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 organisations achievement of meeting its data protection obligations

- a. XXXX
- b. XXXX
- c. XXXX
- d. XXXX
- e. XXXX

5. Performing the audit

- 5.1 The Audit Team Manager responsible for the audit will meet with representatives of XXXX prior to the audit:
- To gain a strategic overview of the management of personal data within the organisation and any relevant background information.
 - To appropriately refine and agree the scope as currently defined.
 - To discuss locations identified by the ICO 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 would seek to visit key departments and sites within the scope of the audit and organisation as arranged with XXXX
- 5.3 In identifying appropriate 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.
- 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.
- 5.5 The audit team will meet with relevant managers and governance staff as appropriate to establish the controls implemented to ensure the organisation complies with its data protection responsibilities. This will be achieved through discussions with staff members, review of relevant records and a review of the procedures in practice.
- 5.6 The ICO will require access to relevant key personnel ‘desk side’ where possible to understand how staff process personal data (limited to the scope provided).
- 5.7 The ICO will consider the extent to which the Internal Audit department include data protection audits in their programmes of audit or compliance work to avoid duplication of work.
- 5.8 As far as is practicable and appropriate the ICO will provide regular feedback on audit progress to the nominated single point of contact. The ICO believes that regular feedback should assist both the ICO and the organisation to quickly understand and address emerging issues, concerns or misunderstanding.

6. Audit team

- 6.1 The following people will be part of the audit team. It is envisaged that XXXX auditors will be used for the on site visit.

XXXX	Team Manager (Audit)
XXXX	Lead Auditor
XXXX	Lead Auditor

7. Reporting

- 7.1 Initially a draft report will be issued detailing the audit findings. Input will be sought from the nominated single point of contact to ensure

that the report is factually accurate. Following any amendments for accuracy a second draft report will be issued complete with any appropriate recommendations. This draft will be returned by XXXX accepting or otherwise the recommendations and including an action plan against each recommendation. Each action will require the title of the person responsible for the action and a date for completion. Thereafter the final report will be issued to agreed recipients.

- 7.2 The audit will provide XXXX with an overall opinion based on the work undertaken, using a framework of four categories of assurance, from high level of assurance to very limited assurance. The 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.
- 7.3 Each of the risks identified in section 4 will be similarly categorised. The rating will take into account the impact of the risk and the probability that the risk will occur.
- 7.4 The ICO will produce an executive summary which it will agree with XXXX.
- 7.5 The Information Commissioner will not proactively publish details of a consensual audit prior to completion of the audit.

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.

XXXX 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.

- 7.6 Dependent on the findings of the final audit report, the ICO may wish to schedule a follow up audit – this would be discussed and agreed with XXXX as appropriate.
- 7.7 The type of follow up activity undertaken will be dictated by the overall assurance provided by the initial audit.
- 7.8 Where the initial assurance level is reasonable, limited or very limited the ICO will produce a follow up report to provide a revised assurance rating, following its review of the actions XXXX has taken to mitigate the risks identified.

- 7.9 The ICO will also produce an executive follow up summary which it will agree with XXXX.

Once the follow up report and executive summary have been completed and agreed the ICO will publish a statement on its website to indicate that a follow up audit has been completed and will seek agreement from the organisation to publish the follow up executive summary.

XXXX 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

	Provided by ICO	Provided by XXXX
Date letter of engagement to be agreed:	Within two working days from date of initial meeting	Within seven working days of receipt
Date of on-site visits:	XXXX	
Date of first draft report:	Within 12 working days from completion of the final site visit	
Date comments on draft provided		Within 10 working days from receipt
Date of second draft:	Within five working days from receipt of first draft with comments	
Date of second draft with action plan:		Within 10 working days from receipt of updated first draft.
Date of final report and executive summary	Five days from receipt of second draft with action plan.	Within five working days from receipt of the executive summary and final report version.

Note that these are provisional dates which may vary with the agreement of both parties.

9. Contacts

9.1 Key contacts

XXXX

XXXX

9.2 A separate schedule of the organisation's personnel to be actively involved with the audit site visits will be documented and agreed between the parties in advance of the site visits.

10. Administration

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

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'. Separate accommodation will also be provided for auditors, where possible, for use while they are not conducting interviews / examinations. No remote network access is required.

11. Expected added value

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

11.2 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.

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

11.4 An improved understanding by the ICO of XXXX, its structure and data protection governance.

Client comments

Agreed by client

Signed:

Position:

Date:



XXXX

Data protection audit report

Final

Auditors: XXXX (Audit Team Manager)
XXXX (Lead Auditor)
XXXX (Lead Auditor)

Distribution:

Draft report: XXXX (XXXX)

Final report: XXXX (XXXX)

Date issued: XXXX

May 2011

Contents

1. Background	page 2
2. Audit opinion	page 4
3. Summary of audit findings	page 5
4. Audit approach	page 6
5. Scope of the audit	page 7
6. Audit grading	page 8
7. Detailed findings & action plan	page 9

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 rests with the management of [insert the company/organisation name].

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.

1. Background

- 1.1 The Information Commissioner may, with the consent of the data controller, assess the extent to which good practice is applied when processing personal data and shall inform the data controller of the results of the assessment. (Data Protection Act (DPA) 1998 s51, (7))
- 1.2 The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach. (Assessment notices code of practice 2.1)
- 1.3 An Assessment notice is the medium through which the Information Commissioner's Office (ICO) will seek to instigate a compulsory audit. However, the Assessment notices code of practice, in the interests of clarity, distinguishes between compulsory and consensual audits. (Assessment notices code of practice, 2.1, Para 6 & Appendix A.)

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual data protection audits.

- 1.4 (This paragraph specific to the circumstances)
- 1.5 **XXXX** has agreed to a **consensual audit** by the ICO of its processing of personal data.
- 1.6 An introductory meeting was held on the **XXXX** with representatives of **XXXX** to identify and discuss the scope of the audit.

2. Audit opinion

- 2.1 The purpose of the audit is to provide the Information Commissioner and **XXXX** with an objective assurance of how **XXXX** are meeting their data protection obligations.
- 2.2 The primary purpose of the audit is to provide the Information Commissioner and **XXXX** with an independent assurance of the extent to which **XXXX**, within the scope of this agreed audit is complying with the Data Protection Act 1998 (DPA).
- 2.3 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall conclusion

Very limited assurance

On the basis of the work that we have performed we consider that the arrangements for data protection compliance in place at **XXXX** at the time, and within the scope, of the audit, with regard to data protection governance and controls, provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore 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)

The audit has identified considerable scope for improvement in existing arrangements and appropriate action has been agreed to reduce the risk of non compliance.

We have made **XXXX** no assurance and **XXXX** limited 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

On the basis of the work that we have performed we consider that the arrangements for data protection compliance in place at **XXXX** at the time, and within the scope, of the audit, with regard to data protection governance and controls, provide limited assurance that processes and procedures are in place and being adhered to.

(Comments specific to audit)

The audit has identified scope for improvement in existing arrangements and appropriate action has been agreed

to reduce the risk of non compliance.

We have made **XXXX** no assurance and **XXXX** limited 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

On the basis of the work that we have performed we consider that the arrangements for data protection compliance in place at **XXXX** at the time, and within the scope, of the audit, with regard to data protection governance and controls, provide reasonable assurance that processes and procedures are in place and being adhered to.

(Comments specific to audit)

The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to reduce the risk of non compliance.

We have made **XXXX** no assurance and **XXXX** limited 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

On the basis of the work that we have performed we consider that the arrangements for data protection compliance in place at **XXXX** at the time, and within the scope, of the audit, with regard to data protection governance and controls, provide high assurance that processes and procedures are in place and being adhered to.

(Comments specific to audit)

The audit has identified 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.

We have made **XXXX** no assurance and **XXXX** limited 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.

3. Summary of audit findings

3.1 Areas of good practice.

XXXX

3.2 Areas for improvement.

XXXX

4. Audit approach

- 4.1 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.
- 4.2 The audit field work was undertaken at **XXXX**, on the **XXXX**.

5. Scope of the audit

5.1 Following pre-audit discussions with **XXXX**, it was agreed that the audit would focus on the following areas:

a. **XXXX**

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 definitions in the table below.

Colour code	Internal audit opinion	Recommendation priority	Definitions
	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified 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.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements
	Very limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore 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

Findings flowing from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Ref	Compliance risk	Issues / findings	Recommended solution	Management comments, responsibility for action and due date
Scope area				
a.				

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

7.6 Any queries regarding this report should be directed to **XXXX**, ICO audit.

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

- **XXXX (XXXX)**

Contents

- 1. Background to follow up assessment**
- 2. Follow up audit opinion**
- 3. Summary of follow up audit findings**
- 4. Follow up audit approach**
- 5. Follow up audit report grading**
- 6. Detailed follow up audit findings**

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 rests with the management of [insert the company/organisation name].

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.

1. Background to follow up assessment

2. Follow up audit opinion

3. Summary of follow up audit findings

Areas of good practice

Areas of improvement

4. Follow up audit approach

- 4.1 When undertaking a follow up assessment the objective is to provide ICO Audit with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks and support compliance with data protection legislation and good practice.
- 4.2 This included a desk based review of evidence provided in relation to XXXX action plan. The evidence reviewed included updated policies and procedures, and XXXX actions to date, an assessment of which demonstrated compliance with XXXX of the recommendations.**
- 4.3 An ICO follow up visit was agreed for the **XX/XX/XXXX** focusing on the verification of the remaining key recommendations.

5. Follow up audit report grading

Follow-up audit reports are graded with an overall assurance opinion linked to the implementation of the agreed audit recommendations. The implementation or otherwise of the recommendations are classified individually to denote their relative importance, in accordance with the definitions in the table below.

Colour code	Internal audit opinion	Recommendation priority	Definitions
	High assurance	Minor points only are likely to be raised	The arrangements provide a high level of assurance that processes and procedures are in place and being adhered to and that the objective of data protection compliance will be achieved. No significant improvements are required.
	Reasonable assurance	Low priority	The arrangements provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that objective of data protection compliance will be achieved.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The achievement of the objective of data protection compliance is therefore threatened. Actions to improve the adequacy and effectiveness of data protection governance and control has been agreed and timetabled.
	No assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide no assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

6. Detailed follow up audit findings

Findings and recommendations from the previous audit have been risk categorised using the criteria defined in Section 5. The rating will take into account the impact of the risk and the probability that the risk will occur in relation to the implementation of the agreed audit recommendations.

For continuity and ease of reference, the findings and recommendations have been numbered in line with the original report and relevant action plan responses.

Ref	Compliance risk	Recommended solution	Management comments, responsibility for action and due date	Current position as at XX/XX/XXXX
Scope area				