

Assessment notices code of practice

Assessment notices code of practice

1. Foreword - signed by the Information Commissioner

I am pleased to present the code of practice for assessment notices in line with the new assessment notice powers available to my office under the Coroners and Justice Act of 2009, which will allow my office to undertake compulsory audits of certain data controllers.

The challenge for the ICO is to become a fully effective, efficient modern regulator, both educating and enforcing to deliver information rights compliance. Audit, I believe has a key role to play in educating and assisting organisations to meet their obligations.

My audit team is developing a risk based approach to help us focus on those organisations that might be striving to comply, but where complaints are significant and where business intelligence highlights the risk of failure. Our engagement with such organisations is normally on a consensual basis

However, there will be instances where this approach alone isn't sufficient, where I will need the power to allow me to undertake 'compulsory' audits in circumstances where there is a risk that individuals' data will be compromised but the organisation is unwilling, for whatever the reason, to engage constructively with my auditors.

This code provides the framework for how such audits will be conducted when an assessment notice has been served on an organisation. It outlines the approach to the audit including opportunities for consultation in relation to the audit report findings and recommendations.

The scope of our extended powers is at the moment relatively modest; as they only apply to government departments. However moving forward it is entirely reasonable to expect that, where the evidence supports it, I will seek to extend my powers to undertake 'compulsory' audits in both the public and private sectors.

I do though recognise that these audit activities may place a burden on data controllers. My staff will endeavour to keep this burden to a minimum, working closely with other regulators and observing the principles of good regulatory practice.

With these new powers of assessment the ICO will ultimately be better placed to provide assurance to individuals that those holding their personal information respect their privacy and do not abuse their trust.



Christopher Graham, Information Commissioner

2. Introduction

2.1 Role of the Information Commissioner

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

Under section 41A of the Act the Information Commissioner may serve certain data controllers with a notice (in the Act referred to as an 'assessment notice') imposing specific requirements on the data controller. The 'assessment notice' is for the purpose of enabling the Information Commissioner to determine whether the data controller has complied or is complying with the data protection principles. For the purpose of this Code this process will be referred to as a 'compulsory' audit.

This code of practice is directed at these 'compulsory' audits.

Data controllers covered by section 41A include government departments, designated public authorities and other categories of designated persons. Any designations will be made by an order made by the Secretary of State.

The Information Commissioner also has a duty under section 51 of the Act to promote the following of good practice among data controllers and to perform his statutory functions in a way that promotes compliance with the Act by data controllers.

Under section 51(7) of the Act the Information Commissioner may, with the consent of a data controller, assess their processing of personal information for the following of good practice. The Information Commissioner must inform the data controller of the results of the assessment. Traditionally the extent of the Information Commissioner's audit activities has been limited to these assessments carried out with consent. For the purpose of this code this process will be referred to as 'consensual' audits.

The process of 'consensual' audits will broadly follow that of 'compulsory' audits and the approach the Commissioner will take will be generally consistent with the provisions of this code. Appendix A covers notable areas of difference.

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. He will usually seek the consent of a data controller to an audit in line with the approach to 'consensual' audits in the first instance. Where however, data controllers are unwilling to engage and risks have been identified the Information Commissioner will use his power to issue an 'assessment notice'.

2.2 Objectives of audit activities

The primary objective of carrying out a 'compulsory' audit is limited to determining the data controller's compliance with the Act's data protection principles. This will include the identification of weaknesses and strengths from a risk mitigation perspective.

Where a 'consensual' audit is undertaken the objective will extend to a data controller's broader following of good practice. Good practice is defined under section 51 (9) of the Act as 'such practice in the processing of personal data as appears to be desirable having regard to the interests of data subjects and other, and includes (but is not limited to) compliance with the requirements of this Act'.

The standards against which compliance will be judged will be the legal requirements of the Act as amplified in the Information Commissioner's Office's (ICO) 'The Guide to Data Protection' together with other relevant ICO codes and guidance.

In light of experience of how these audits work in practice, the Information Commissioner will consider additional common standards to be referred to by his staff when assessing data controllers. These will be referenced in the subsequent revisions of this code, the first of which will be produced within two years of initial publication (see 2.4 below).

2.3 Risk-based approach

In line with the Regulators' Compliance Code the Information Commissioner will adopt a risk-based, proportionate and targeted approach to audit activities. This approach will be refined in the light of the ICO's developing audit experience.

To identify high-risk data controllers and sectors he will use:

- business intelligence such as news items;
- data controllers' annual statements on control;
- data controllers' information security maturity models;
- information received from other regulators;
- 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.

2.4 Code of practice (the code)

The Information Commissioner is required to prepare and issue this code under section 41C of the Act. The code must address the manner in which the Information Commissioner's functions in connection with 'assessment notices' are to be exercised.

The requirements of the code are directed at the Information Commissioner himself and provide guidance and reassurance for data controllers who are subject to 'assessment notices' and 'compulsory' audits.

The Information Commissioner is committed to keeping the code up to date to reflect changes in auditing standards and practices and may amend the code where appropriate; for example in the light of practical experience or as a result of legislative changes. The code, in any case, will be reviewed within two years of publication or if further designation extends the Information Commissioner's powers to conduct 'compulsory' audits outside the public sector.

In line with section 41C of the Act the code may only be issued, altered or replaced with the Secretary of State's approval.

The code will be made publicly available via the Information Commissioner's website.

2.5 Scope of the code

This code sets out the factors that will inform the Information Commissioner's decision to serve an assessment notice on a data controller and specifies amongst other things how 'compulsory' audits will be conducted with reference to:

- documents and information that are to be examined or inspected;
- documents and information that are **not** to be examined or inspected;
- the nature of inspections and examinations;
- the nature of interviews to be carried out; and
- the preparation, issuing and publication by the Information Commissioner of assessment reports produced by auditors.

3. 'Assessment notices'

3.1 Factors to be considered before issuing notices

'Assessment notices' will be served where it is deemed necessary by the Information Commissioner because:

- a risk assessment has been conducted and indicates a probability that personal data is not being processed in compliance with the Act together with a likelihood of damage or distress to individuals, and
- the data controller has failed to respond to a written request from the Information Commissioner to undertake an audit or has refused consent to such an audit, without adequate reasons.

In determining the risks of non compliance the Information Commissioner will consider one or more of the following factors:

- The compliance 'history' of the data controller based on complaints made to the 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.
- 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 Information Commissioner will consider the following factors:

- The number of individuals potentially affected.
- The nature and sensitivity of the data being processed.
- The nature and extent of any likely damage or distress caused by non compliance.

Additionally the Information Commissioner may also serve an assessment notice:

- Where there is a need to be assured that a data controller has taken appropriate measures to comply with a formal undertaking or enforcement notice he has issued or
- Where he has been given a specific responsibility for scrutiny such as the Cabinet Office's 'Data Handling Procedures in Government: Final Report' or where given in similar public commitments by data controllers.

Details of 'assessment notices' will be published on the Information Commissioner's website.

3.2 The content of notices

- 'Assessment notices' will be issued in compliance with sections 41A (3), 41A (5), 41A (6) and 41B (1) of the Act which state that the Information Commissioner must tell the data controller of the specific requirements for a particular assessment, such as which premises are to be entered or which equipment is to be inspected and when. It must also tell them of their rights of appeal under section 48 of the Act. Any appeal (Appendix B Annex 2) must be made to the First-tier Tribunal (Information Rights) within 28 days of the date on which the assessment notice was served. An audit cannot take place until this 28 day time period has elapsed.
- Where the Information Commissioner decides that the data controller must comply urgently with a notice then as required under section 41B (2) of the Act, the notice will state it is a matter of urgency and why. In such instances the audit cannot begin until seven days after the day on which the notice is served.

- The Information Commissioner will only use the 'urgency' option when there are reasonable grounds for believing that there is a high probability of significant non-compliance with the Act with serious associated risks to individual privacy.

An example of a notice can be found in Appendix B.

A covering letter, to the notice, will identify the purposes, objectives and scope of the 'compulsory' audit. It will also identify any requests for additional assistance which, in the view of Information Commissioner, will facilitate the effective conduct of the audit. By way of example this might include the identification, by the data controller, of a 'single point of contact' and, access to staff, other than those processing personal data with roles in personal data assurance or governance.

3.3 The cancellation of notices

The Information Commissioner may cancel an 'assessment notice' if a data controller satisfactorily explains why, in the circumstances, the proposed audit assessment should not take place or where there is a legitimate request for postponement.

Where a request is made for a postponement the Information Commissioner will require the data controller to submit alternative dates. If agreement cannot be reached on alternative dates then the notice will stand but may be subject to appeal (see section 3.2 above).

The Information Commissioner may also cancel an audit where there are circumstances beyond his control which are likely to impact on the successful completion of the audit.

The data controller will be advised in writing of any cancellation and the reasons. Details of any cancellations will also be published on the Information Commissioner's website.

3.4 Rights of appeal

As set out at 3.2 above, data controllers have a right of appeal to the First-tier Tribunal (Information Rights) against any of the terms of an 'assessment notice'.

Such an appeal must be made within 28 days of an 'assessment notice' being served and full details of appeal rights and how to make an appeal will be included in the assessment notice. These are included in this code at Annex 2 to Appendix B.

It is important to note that failure to comply with the terms of an 'assessment notice' will be grounds for a judge to issue a warrant for entry and inspection to the Information Commissioner under Schedule 9 to the Act. This will enable the Commissioner to enter the premises specified in the 'assessment notice' for the purpose of determining whether the data controller has complied or is complying with the data protection principles.

Where the Information Commissioner determines that a data controller must comply urgently with an 'assessment notice' an appeal must be made within seven days of the notice being served. Here the right of appeal is against the 'urgency' requirement rather than the full terms of the notice.

4. Conduct of 'compulsory audits'

4.1 Auditors

Audits will be conducted by competent auditors employed directly by the Information Commissioners Office (ICO) or contracted to, and under the control of, the ICO. Auditors will have, or be working to, an audit qualification and a relevant qualification in data protection.

Auditors on occasion may be accompanied by other ICO staff with specific experience or knowledge of devolved government powers.

Auditors and accompanying ICO staff will sign confidentiality clauses as part of their contract of employment and engagement. They will be subject to section 59 of the Act which makes it a criminal offence for them to disclose information obtained during the course of their duties without lawful authority.

Auditors and accompanying ICO staff will also be prepared to sign confidentiality agreements with data controllers where those agreements do not unreasonably restrict the ICO in fulfilling its regulatory functions.

Auditors and accompanying ICO staff will be subject to the Official Secrets Act 1989.

4.2 Audit process

Audits undertaken by the Information Commissioner will be conducted in two phases; an 'adequacy' audit and a 'compliance' audit.

The 'adequacy' audit will normally be conducted off site and will consist of a review of relevant policies, procedures, guidance and training material. The key consideration will be how these documents provide a framework for delivering compliance with the Act. Any significant findings will be detailed in the Audit Report. These documents and the output from the review will provide the framework for the 'compliance' audit.

The length of time necessary to conduct the 'adequacy' audit will vary based on the volume and complexity of material provided in response to the notice.

The 'compliance' audit will be focused on the agreed scope and conducted on the data controller's site(s) over a number of days. Evidence of compliance with the data protection principles, the following of good practice and adherence to policies will be gathered through meetings with staff and the observance of personal data handling processes.

The number of 'on site' days will vary based on the scope, the organisational structure and the location of sites. For the majority of staff, identified for interview, then not more than an hour of their 'face to face' time will be required. The Information Commissioner will take all reasonable steps necessary to minimise the impacts on normal business activity.

The findings of the audits will be documented in an audit report with opportunities provided for the data controller to comment on accuracy and respond to the recommendations. Informal feedback on preliminary findings may also be provided by auditors during the course of an audit.

4.3 Documents and information

Access will be required to the specified documents and information, or classes of documents and information, which define and explain how the data controller intends to meet his obligations under the Act and the governance controls in place to measure compliance. This could include for example:

Strategies	Policies	Procedures
Guidance	Codes of Practice	Training Material
Protocols	Frameworks	Memoranda of Understanding
Contracts	Privacy Statements	Privacy Impact Assessments
Control Data	Job Descriptions	Terms of Reference

Access may also be required to specified personal data, or classes of personal data, and to evidence that it is being handled in compliance with the policies and procedures in as much as they deliver compliance with the Act. The level of such access will be proportionate to that required to assess compliance.

As provided for by section 41B (3) of the Act access will not be required to information which is subject to legal privilege. Access will also not be required to information which:

- has a high level of commercial sensitivity;
- is exempt information for the purposes of the Freedom of Information Act 2000 by virtue of section 23 of that Act (information supplied by, or relating to bodies dealing with security matters); or

- is exempt from Part V of the Data Protection Act by virtue of a certificate under section 28 (national security).

The Information Commissioner recognises that there might also be legitimate concerns about other information which relates to issues of national security, international relations or sensitive activities and in such cases anticipates that it will generally be possible to audit data protection compliance without access to such information.

The Information Commissioner will listen to representations from data controllers in respect of any 'assessment notice' which requires access to such information with a view to limiting access to the minimum required to adequately assess the compliance of a data controller and to meeting any reasonable conditions the data controller may wish to impose in relation to access. Such representations should be made within 28 days of the notice date.

Where necessary and appropriate, the ICO will ensure that properly vetted staff are made available to inspect such information. In any case, access to information classified as restricted or above, with the exception of the previous paragraphs will be limited to ICO staff with Security Check clearance or above.

There may be a requirement to view health and social care records. The confidentiality of such data will be respected and any such access will be limited to the minimum required to adequately assess compliance by the data controller. The content of such records will not be taken off site, copied or transcribed into working notes and will not be presented in any reporting of the assessment.

The extent to which other information is taken off site will be kept to a minimum and such information will only be retained by the ICO so far as it is necessary to complete the audit and any identified follow up action.

4.4 Inspections and examinations

Inspections and examinations are key review elements of the audit. They identify objective evidence of compliance and how policies and procedures have been implemented and effectively mitigate data protection risk.

These reviews of personal data, and associated logs and audit trails, may consider both manually and electronically stored data including data stored centrally, locally and on mobile devices and media.

The reviews will be used to evaluate how a data controller:

- obtains, stores, organises, adapts or alters information (e.g. policies and procedures) or personal data;
- retrieves, consults, or uses the information or personal data;
- discloses personal data by transmitting or disseminating or otherwise making the data available; and

- weeds and destroys personal data.

In addition the reviews may cover management/control information used to monitor and record how personal data is being processed and measure how a data controller meets its obligations under the Act.

The review may evaluate physical and IT-related security measures including how personal data is stored and disposed of.

The review and evaluation process may take place in situ as part of a discussion with staff to demonstrate 'practice' or independently by way of sampling by auditors. If information is held electronically the data controller may be required to provide manual copies or facilitate direct access.

Any direct access would be limited to the identified records, would only be done locally and would be for a limited and agreed time.

Data reviewed as part of the review and evaluation process but not specifically identified in the assessment notice may only be taken off the data controller's site with the data controller's permission.

4.5 Interviews

Interviews will comprise discussions with the:

- data controller's staff and contractors;
- data processor's staff; and
- staff of relevant service providers as specified in the assessment notice.

Discussions will be conducted to further develop an understanding of working practices and / or awareness of data protection considerations. Departmental managers, operational staff, support staff (e.g. IT staff, security staff) as well as staff involved with information and data protection governance may be considered as interview candidates.

Discussions will be scheduled and agreed with the data controller before the on-site audit takes place. A schedule of areas to be covered will be provided to the data controller prior to the audit and the level and grade of staff e.g. managers, operational staff etc will be discussed and agreed. Individuals should be advised, by the data controller, in advance of their required participation.

Key control questions will be used to understand individual roles and the processes followed or managed specifically with reference to the handling of personal data and the security of that data. Some questions may relate to data protection training and awareness but they will not be framed as a test nor are they intended to catch people out.

Interviews may be conducted at an individual's desk or in a separate room dependent upon circumstances and whether there is a need to observe the working environment or examine information and records. Interviews will normally be 'one-to-one' but sometimes it may be appropriate, because for example of shared responsibilities, to include a number of staff in an interview. Notes will be taken by the auditors during the interviews.

Given the nature of interviews the Information Commissioner does not consider it to be necessary for those subject to interview to be accompanied by third parties but he will not object where it is reasonably recommended.

Every effort will be taken to restrict interviews to staff identified within the agreed schedule but where it is clear in the course of the audit that access to additional staff may be necessary to address unresolved questions this will be arranged with the consent of the data controller. In a similar way the schedule should not preclude confirmatory conversation with a consenting third party; for example where the third party is in close proximity to a desk side discussion.

Interviews are to help in assessing compliance. They do not form part of, or provide information for, any individual disciplinary or criminal investigation. Should evidence of criminal activity by an individual emerge during an interview, the interview will be halted.

Individuals' names may be used in distribution lists and acknowledgements sections of reports but will not be referenced in the body of any report. Job titles may be used where appropriate.

5. Audit reporting

5.1 The audit report

Section 41C of the Act refers to the reports stemming from an assessment, (to include, amongst other things, determinations and recommendations) as 'assessment reports'. For the purpose of this Code, these reports will be referred to as 'audit reports'.

The audit report gives an audit opinion as to whether or not a data controller has complied or is complying with the data protection principles. It will further report levels of assurance, against the prescribed scope and identified risks, in respect of the mitigating measures and controls implemented by the data controller.

The findings will be presented by way of:

- a summary of findings;
- an audit opinion;
- detailed findings against predefined risks; and
- associated recommendations.

The report will include an opinion based on the assessment and audit work that the Information Commissioner's staff have performed. The opinion will consider the governance and associated control arrangements in place at the time of the audit and provide a statement on the status of the data controller's compliance with the data protection principles.

Where it is identified in the course of an audit that the data controller has failed in any way to meet the requirements of the assessment notice the Information Commissioner will make a decision as to the material impact on the audit and consequently whether reference will be made to the omission in the report.

The report will also include recommendations as to any steps which the data controller ought to take or not take to comply with the data protection principles. In line with the principles of better regulation the recommendations will be risk rated, on the ground of impact and probability, to identify those needing immediate or urgent action.

A draft report will initially be presented to the data controller to enable it to comment on the factual accuracy of the report and to highlight any pertinent information which might have been omitted. The data controller will be requested to comment on the recommendations and identify who should act on them.

The Information Commissioner will address any issues identified by the data controller's feedback and update the audit report as appropriate. The report will include the data controller's comments on the Information Commissioner's recommendations. These may include points of difference which cannot be resolved between the data controller and the Information Commissioner.

If the data controller fails to respond to the draft report and recommendations within reasonable and defined timescales then the Information Commissioner will issue the report as a final report and present it to the Chief Executive Officer / Accounting Officer.

In addition to the audit report an 'executive summary' report for publication will be produced by the Information Commissioner's staff providing a précis of the audit background, scope, key findings and compliance considerations and an overall audit opinion. The data controller will be provided with a copy of the 'executive summary' report prior to the publication and have an opportunity to comment.

5.2 Report publication

Following the completion of the audit, basic details of the audit and the 'executive summary' reports will be made available for a year on the Information Commissioner's website. The Information Commissioner will previously have taken into account any opinions from the data controller about the suitability for publication of any element.

'Executive summary' reports may still be available on request afterwards and whilst they continue to be retained in line with the Commissioner's retention policy.

The Information Commissioner will also provide support for links to the data controller's own websites should the data controller request the option of making a formal response to the report available.

Requests made for copies of the full audit report, made under the Freedom of Information Act 2000, will be considered, on a case by case basis, in line with the Information Commissioner's obligations as a public authority. In such instances the Information Commissioner will seek the views of the data controller on disclosure, specifically with reference to matters such as possible prejudice to information security or commercial confidentiality.

The Commissioner may also make general references to assessments and the conclusions drawn from them in his annual or other reports.

6. Actions resulting from an Audit

The Information Commissioner does not intend that audits will normally lead to formal enforcement action; rather they are seen as a means of encouraging compliance and good practice. However, on issuing the final report the Information Commissioner will indicate whether it is his intention to follow up on the data controller responses to his recommendations, if any. Follow up may be by way of seeking, from the data controller, written assurances of actions taken or a further audit.

However, the Information Commissioner cannot give absolute assurances that enforcement action will not be taken as a result of an audit as to do so would require him not to act, even where significant risks to individuals have been identified. He must reserve the right to use his powers in the case of any identified major non-compliance where the data controller refuses to address a recommendation within an acceptable timescale.

As stated in the Information Commissioner's published guidance on monetary penalties and as required under section 55A subsection (3) of the Act, the Information Commissioner cannot impose a monetary penalty on a data controller where a contravention was discovered in the course of carrying out an audit.

7. Quality assurance

The Information Commissioner will establish internal arrangements to ensure that audits are managed and conducted consistently in compliance with this Code. Audits conducted by the Information Commissioner and the associated processes will be subject to ongoing internal quality assurance reviews.

8. Summary of Audit Process

A flowchart summarising the audit process as a whole can be found in Appendix C.

Appendix A – ‘Consensual’ audits

1. The Information Commissioner’s approach

The approach the Information Commissioner takes to ‘consensual’ audits will as far as practicable be the same as that for compulsory audits. However there are differences in the process of engagement, where no ‘assessment notice’ will be issued, and in the arrangements for publication of the ‘executive summary’ report. These differences are explained below.

2. Engagement

Data controllers will initially be informed in writing of the Information Commissioner’s intention to conduct a ‘consensual’ audit. This letter will explain the audit process and the basis on which they have been selected. It will include a broad outline of the intended scope, a provisional list of required polices and procedures and the projected dates of the various audit activities.

The Information Commissioner will consider representations from data controllers in respect of the necessity of an audit, the timing of an audit or the proposed scope of an audit. Where there is a clear indication from a data controller that they are unwilling to participate in a ‘consensual audit’ the Information Commission will consider any written representations in determining whether it is appropriate, in all the circumstances , to serve an ‘assessment notice’.

Where there is agreement in principle to an audit the Information Commissioner will work closely with the data controller, through a single point of contact, in advance of any on site audit activity. This will enable the scope to be further refined, the potential participants identified and a timetable of activities to be agreed. Furthermore, this work should help the data controller in managing communication with its own staff members.

The Information Commissioner will send a formal ‘Letter of Engagement’ (see illustrative example in the annex to this appendix) following discussions with the data controller and prior to the ‘compliance’ audit starting. The letter will define the agreed scope of the audit and the audit objectives, both of which are primarily based on compliance with the eight data protection principles in the Act. It will also include timescales, provide details of the Information Commissioner’s staff to be employed on the audit and cover any special factors which may relate to a particular audit.

The Letter of Engagement will also detail any documents and information required by the audit team for its conduct of the ‘adequacy’ audit. Access to such documents and information, subject to the data controllers consent, may be requested in advance of the formal signing of the ‘Letter of Engagement’ to expedite the ‘adequacy’ audit.

The data controller will be able to comment on the 'Letter of Engagement' before signing. If agreed by both parties, reasonable changes may be made to the 'Letter of Engagement' during the audit process.

If there is a failure to agree to a 'consensual audit' at any stage of this process, the Information Commissioner will determine whether it is necessary, in all the circumstances, to conduct a 'compulsory' audit (see section 3.1).

3. Audit reporting and publication

The Information Commissioner will not proactively publish details of any 'consensual' audit prior to completion of the audit.

As with 'compulsory' audits both a full audit report and an 'executive summary' report will be produced and will be subject to a validation process. Whilst the Information Commissioner will encourage the publication of 'consensual audit' 'executive summary' reports, data controllers may choose not to do so. Where this is the case the website will indicate that the report has been withheld.

Requests made for copies of unpublished 'executive summary' audit reports or the full audit reports made under the Freedom of information Act 2000 will be considered with on a case by case basis in line with the Information Commissioner's obligations as a public authority.

Annex 1 to Appendix A - sample letter of engagement

AUDIT LETTER OF ENGAGEMENT

To:

CC:

Date:

From: Information Commissioner's Audit Group

1. **Background** – (i.e. general information about a specific programme of work or matters directly relating to the organisation and factors which may have been taken into account in selecting the data controller for audit e.g. reference to any external consultants' reports, internal statements on control, self reported breaches, or undertakings / enforcements).
2. **Purpose and objectives** – (i.e. why the ICO is undertaking the audit and what it is seeking to achieve)
 - 2.1 The purpose of the audit is to provide the 'data controller' and the Information Commissioner with an assessment of how the 'data controller' is meeting its data protection obligations.
 - 2.2 The primary objective of the audit is to provide the Information Commissioner with a level of assurance that personal data is adequately protected and that privacy considerations are being appropriately engaged.
3. **Scope** – (i.e. areas to be covered during the audit linked to areas of highest risk)
 - 3.1 The Audit scope will focus on specific processes and activities to assess how their implementation contributes to compliance with the data protection principles within the following areas:
 - a. Data Protection Governance – with specific reference to the controls used to measure and report compliance with the Data Protection Act 1998 (the Act).
 - b. The provision and monitoring of staff training and awareness of data protection requirements, relating to their roles and responsibilities.
 - c. The processes in place to ensure adequate security is applied to the 'data controller's' IT systems, including portable and mobile devices, to ensure the appropriate storage and use of personal data.

- d. The processes in place to ensure adequate physical security is applied to the storage and use of manual files, both inside and outside the 'data controller's' premises.
- e. The processes in place to ensure Subject Access Requests are dealt with appropriately, in compliance with data protection legislation.

Out of Scope – (i.e. areas not to be included in the audit along with some information as to why the area isn't to be included)

- 3.2 The audit will not specifically review policies and procedures in respect of data transfers, outside of the European Economic Area. However, the ICO retains the right to comment on any weaknesses observed in these areas in the course of the audit that could compromise good data protection practice.

- 4. **Risks** – (i.e. those risks that may impact on the achievement of compliance in the areas identified under the scope with specific reference to risks where non compliance may result in damage to both individuals and the organisation.)

- a. A failure to identify and implement controls by which compliance with data protection can be measured and reported, raises the risk of the 'data controller' being unaware of whether it is meeting its obligations, resulting in poor data protection practice or potential breaches of the Act not being identified or addressed.
- b. A failure to provide and implement staff training and awareness regarding the correct use and management of personal records raises the risk of loss or inappropriate usage of data, with the potential to cause damage and distress to individuals, and reputational damage to the 'data controller'.
- c. A failure to implement security measures which adequately protect electronically held personal data raises the risk of loss, damage or inappropriate access to data leading to distress to the affected individuals, reputational damage to the 'data controller' and non-compliance with the Act.
- d. A failure to appropriately control and secure manual personal data both within and outside the 'data controller's' premises raises the risk that personal data will be lost, damaged or inappropriately disclosed, resulting in distress to the individual and non-compliance with the Act.
- e. A failure to ensure Subject Access Requests are dealt with appropriately raises the risk that an individual's rights to

information may be compromised resulting in distress to the individual and non-compliance with the Act.

5. Performing the audit – (i.e. who – ICO Auditors, where – the locations relating to the organisation, and how – reference to the schedule of activities and the importance of a single point of contact)

5.1 The audit will be undertaken by ICO Auditors, on site, at the agreed locations.

5.2 The on-site audit will collect evidence to assess compliance with the ‘data controller’s’ own policies and procedures and with the requirements of good data protection practice. This will be achieved through discussions with relevant staff members and the review of processes and procedures related to the use of personal data.

5.4 A schedule of activities will be agreed with the ‘data controller’s’ nominated single point of contact for the Audit.

6. Documentation

6.1 The ‘data controller’ will initially arrange the provision of policies, procedures, guidance, governance reports and training material relevant to the scope of the audit as requested for preparation of on-site audit visits.

6.2 The audit work will be documented according to the Information Commissioner’s Office (ICO) Audit Group standards.

7. Internal Audit team

7.1 The Audit team will comprise of the staff as detailed below:

	Audit Team Manager
	Compliance Auditor
	Compliance Auditor
	Compliance Auditor

8. Reporting – (i.e. the reporting process and circulation for each of the report stages)

- 8.1 A first draft report will be issued to named recipients within the organisation to agree the factual accuracy of the report. A second draft report will then be issued which the data controller may choose to circulate more widely to gain agreement on the audit recommendations.
- 8.2 Thereafter, a final report will be distributed which will include the 'data controller's' responses to, owners of, and implementation dates for the agreed recommendations.
- 8.3 The 'data controller' will be provided with an audit opinion based on the work undertaken. The opinion will be based on an independent assessment of the processes and procedures to mitigate the risks identified.
- 8.4 Audit recommendations will be risk categorised using the red, amber, yellow, green criteria, with red being high priority and green low priority. The rating will take into account the impact of the risk and the probability that the risk will occur.
- 8.5 An 'executive summary' report will be produced based on the final audit report. This will be published on the Information Commissioner's website with agreement of the 'data controller'.

9. Timescales

Date letter of engagement to be agreed:	Within one week of receipt by 'data controller'
Date of on-site visit (s):	Normally 3 days duration
Date of visits to satellite offices: (if appropriate)	
Date of Audit draft report:	Within 10 working days of audit visit
Date of Audit final report:	Within 10 working days of receipt of agreed second draft

10. Contacts

- 10.1 Key contact(s) within the organisation (As agreed and including the nominated single point of contact).
- 10.2 A separate schedule of on site interviews with the 'data controller's' relevant staff will be documented and agreed between the parties in advance.
- 10.3 Access to staff from the 'data controller's' third party service providers may also be required.

11. Administration

- 11.1 Individual site arrangements for access and audit will be organised through the key contact.
- 11.2 Where possible staff interviews will be carried out 'desk side'.
- 11.3 A room will be made available to the Information Commissioner's auditors at sites identified in the schedule to carry out interviews when it is not appropriate to do so 'desk side'.
- 11.4 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.

12.1 Expected Added Value

- 12.1 The provision of an independent assurance in relation to compliance with the Act.
- 12.2 The opportunities for staff to discuss and exchange relevant data protection issues with the members of the Information Commissioner's audit team.
- 12.3 The data protection knowledge and experience of the auditors enables a proportionate consideration of the risk and impact of non-compliance to be taken.

Client Comments		
Agreed by Client	Yes/No	
Signed:	Position:	Date:

NOTE – The scope, risks and time scales in this document are provided for illustrative purposes only and would be subject to agreement with the data controller.

Appendix B – Assessment Notice

**THIS IS AN IMPORTANT DOCUMENT. IT AFFECTS YOU.
PLEASE READ IT CAREFULLY.**

**THE DATA PROTECTION ACT 1998 (PART V, SECTION
41A)**

ASSESSMENT NOTICE

DATED [*Insert date*]

To: [*Data controller*]

Of: [*Address*]

1. [*Insert legal name of data controller*] is a "data controller" as defined in section 1(1) of the Data Protection Act 1998 (the "Act") and is referred to in this Notice as the data controller.
2. In order to conduct an Audit for the purpose of enabling the Information Commissioner (the "Commissioner") to assess whether the data controller has complied or is complying with the data protection principles at Part I of Schedule 1 to the Act, the Commissioner requires you to comply with the requirements set out in Annex 1 within the time(s) specified.

References to the Commissioner in this Notice include references to the Commissioner's officers and staff.

3. Attached to Annex 1 are:
 - (i) copies of correspondence constituting the steps that have been taken by the Commissioner to assess any processing of personal data with the consent of the data controller under section 51(7) of the Act.
 - (ii) A copy of the code of practice as to the manner in which the Commissioner's functions under section 41A of the Act are to be exercised.
4. **In view of the matters referred to above, the Commissioner hereby gives notice that in exercise of his powers under section 41A of the Act he requires that the data controller shall comply with the requirements set out in Annex 1 within the time specified.**

Right of Appeal

There is a right of appeal against this Notice to the First-tier Tribunal (Information Rights) (the "Tribunal"). If an appeal is brought the requirements set out in Annex 1 of this Notice need not be complied with pending the determination or withdrawal of the appeal. Information about appeals is set out in the attached Annex 2.

Any Notice of Appeal should be served on the Tribunal within 28 days of the date on which this Notice is served. If Notice of Appeal is served late the Tribunal will not accept it unless it is of the opinion that it is just and right to do so by reason of special circumstances.

Information concerning further statutory provisions relating to this Notice is set out in Annex 3.

Dated:

Signed:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Annex 1 to Appendix B

THE DATA PROTECTION ACT 1998 (PART V, SECTION 41A)

REQUIREMENTS

1. The data controller is required to permit the Commissioner to enter the premises specified in the table below.

Premises	Time/ Period

2. The data controller is required:

- (i) to direct the Commissioner to any documents on the premises described in the table below;
- (ii) to permit the Commissioner to inspect or examine any of the documents to which the Commissioner is directed;
- (iii) to comply with any request from the Commissioner for a copy of any of the documents to which the Commissioner is directed.

Description of document	Time/Period

3. The data controller is required:

- (i) to assist the Commissioner to view any information described in the table below that is capable of being viewed using equipment on the premises;
- (ii) to permit the Commissioner to inspect or examine any of the information to which the Commissioner is assisted to view;
- (iii) to comply with any request from the Commissioner for a copy (in such form as may be requested) of any of the information which the Commissioner is assisted to view.

Description of information	Time/Period

4. The data controller is required:

- (i) to direct the Commissioner to any equipment or other material on the premises which is described in the table below;
- (ii) to permit the Commissioner to inspect or examine any of the equipment or material to which the Commissioner is directed.

Description of equipment/other material	Time/Period

5. The data controller is required to permit the Commissioner to observe the processing of personal data that takes place on the premises.

Processing	Time/Period

6. The Commissioner requires that the data controller makes available for interview the persons of the specified descriptions described in the table below who process personal data on behalf of the data controller and are willing to be interviewed.

Person descriptions	No of persons	Time/Period

Annex 2 to Appendix B

THE DATA PROTECTION ACT 1998 (PART V, SECTION 48)

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Act gives any person upon whom an assessment notice has been served a right of appeal to the First-tier Tribunal (General Regulatory Chamber) (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers: -

- a) that the notice against which the appeal is brought is not in accordance with the law; or
- b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

GRC & GRP Tribunals
PO Box 9300
Arnhem House
31 Waterloo Way
Leicester
LE1 8DJ

- a) The notice of appeal must be served on the Tribunal within 28 days of the date on which notice of the Commissioner's decision was served on or given to you.
- b) If your notice of appeal is late the Tribunal will not accept it unless it is of the opinion that it is just and right to do so by reason of special circumstances.
- c) If you send your notice of appeal by post to the Tribunal, either in a registered letter or by the recorded delivery service, it will be treated as having been served on the Tribunal on the date on which it is received for dispatch by the Post Office.

4. The notice of appeal should state: -
- a) your name and address;
 - b) the decision which you are disputing and the date on which notice of the decision was served on or given to you;
 - c) the grounds of your appeal;
 - d) whether you consider that you are likely to wish a hearing to be held by the Tribunal or not;
 - e) if you have exceeded the 28 day time limit mentioned above the special circumstances which you consider justify the acceptance of your notice of appeal by the Tribunal; and
 - f) an address for service of notices and other documents on you.

In addition, a notice of appeal may include a request for an early hearing of the appeal and the reasons for that request.

5. By virtue of section 41B (1) of the Act, an assessment notice may not require any of the requirements imposed by the notice to be complied with before the end of the period in which an appeal can be brought and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.
6. However, section 41B (1) of the Act does not apply where the notice contains a statement that the Commissioner considers that the notice should be complied with as a matter of urgency.
7. Section 48(3) of the Act provides that where an assessment notice contains a statement that the notice should be complied with as a matter of urgency then, whether or not you intend to appeal against the notice, you may appeal against -
- (a) the Commissioner's decision to include the statement in the notice, or
 - (b) the effect of the inclusion of the statement as respects any part of the notice.
8. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

9. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Act, and the Tribunal (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 L.20).

Annex 3 to Appendix B

THE DATA PROTECTION ACT 1998 (PART V, SECTION 41A)

ASSESSMENT NOTICES – FURTHER STATUTORY PROVISIONS

STATUTORY LIMITATION TO COMPLY WITH THE REQUIREMENTS IMPOSED IN AN ASSESSMENT NOTICE

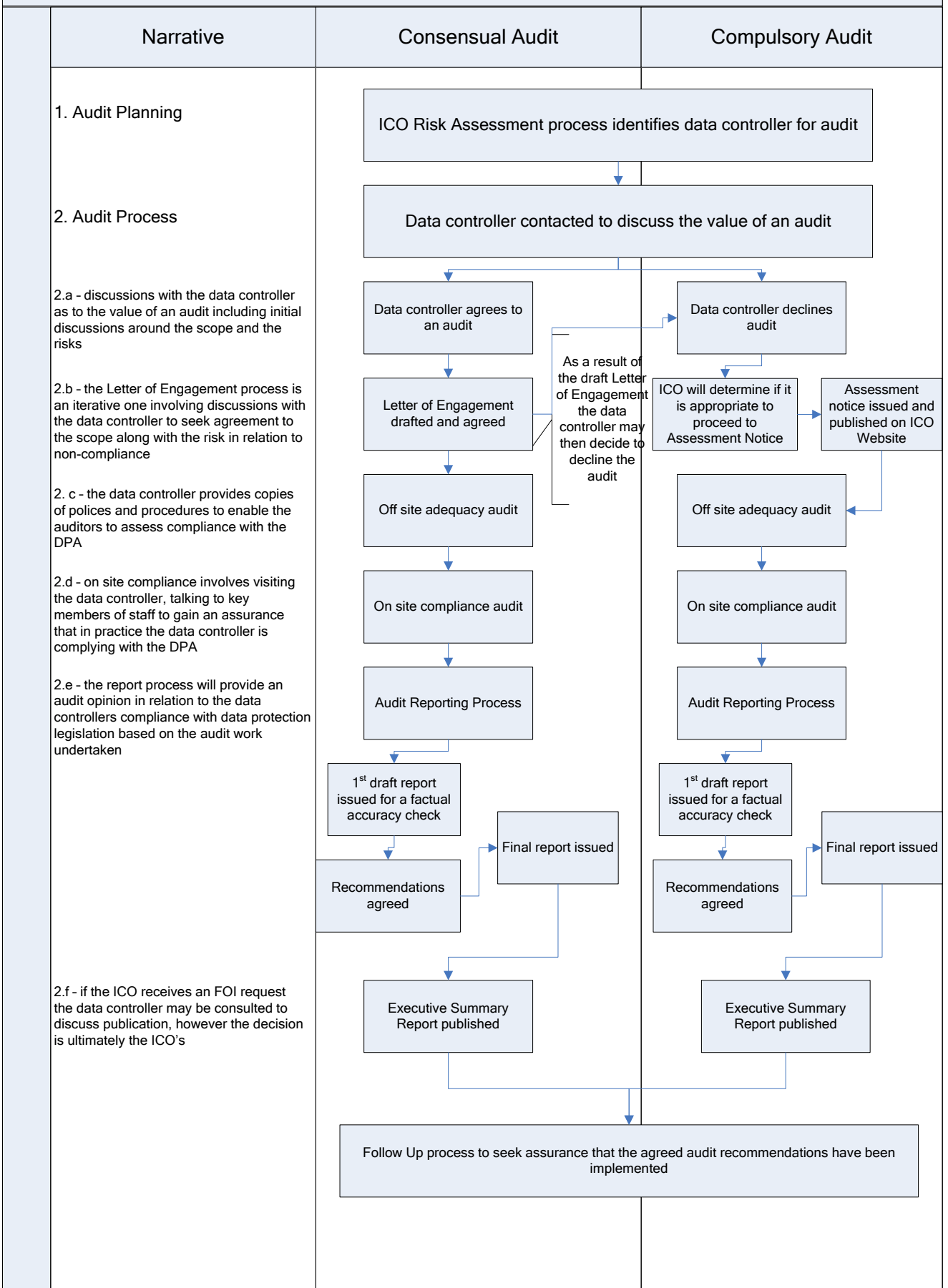
(1) Section 41B (3) of the Act provides that:

“A requirement imposed by an assessment notice does not have effect in so far as compliance with it would result in the disclosure of-

- (a) any communication between a professional legal adviser and the adviser’s client in connection with the giving of legal advice with respect to the client’s obligations, liabilities or rights under this Act, or
- (b) any communication between a professional legal adviser and the adviser’s client, or between such an adviser or the adviser’s client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the Tribunal) and for the purposes of such proceedings.”

(2) Section 41B (4) of the Act provides that:

“In subsection (3) references to the client of a professional legal adviser include references to any person representing such a client.”



Find out more

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

t: 0303 123 1113
w: www.ico.gov.uk

April 2010