



Information Commissioner's Office (ICO)

Consultation on the Assessment Notices Code of Practice 10 February 2010

A Code of Practice for Assessment Notices will be published in April 2010 in line with the extended data protection audit powers available to the Information Commissioners Office under the Coroners and Justice Act of 2009. The Code will provide the framework for how audits will be conducted when an Assessment Notice has been served on an organisation. It will outline the approach to the audit including opportunities for consultation in relation to the audit report findings and recommendations.

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

A draft code for consultation is published today on the [consultations pages](#) of our website. The Information Commissioner would like to hear the views of stakeholders before the consultation closes on 24 March 2010. Please send comments and suggestions either:

by email to: Chris.turner@ico.gsi.gov.uk

Or by post to:

Chris Turner,
Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow, SK9 5AG

Whilst we will not be able to reply to each comment, all views will be considered and we will publish a summary of our responses to the comments we receive

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 extended data protection audit powers available to my office under the Coroners and Justice Act of 2009.

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.

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 Code of Practice (the Code)

The Information Commissioner is required to prepare and issue this Code under section 41C of the Data Protection Act 1998 (the Act). 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.

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 only applies when the Information Commissioner decides to issue an assessment notice.

2.2 Scope of the Code

The 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 carried out; and
- the preparation, issuing and publication by the Information Commissioner of assessment reports produced by auditors.

Information relating to the Information Commissioner's wider risk based approach to audit and engagement with data controllers is included in this Code to provide relevant background information and a context for the assessment activity.

2.3 Role of the Information Commissioner

The Information Commissioner is responsible for enforcing and promoting compliance with the Act.

The Information Commissioner has a duty under section 51 of the Act to promote the following of good practice among data controllers and also 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; this in practice has been provided by way of a report.

Traditionally the extent of the Information Commissioner's audit activities has been limited to audits carried out with consent – 'consensual audits'.

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

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

The Information Commissioner primarily intends to use his power to issue assessment notices where risks are identified and data controllers are unwilling to engage voluntarily.

2.4 Assessment auditors

'Compulsory audits' will be conducted by competent auditors employed directly by the Information Commissioners Office (ICO) or directly contracted to the ICO.

Auditors 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.

2.5 Quality assurance

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

3. ICO audits - background

3.1 Objectives

The primary objectives for carrying out audit activities are to assess a data controller's conformity with good practice and to determine compliance with the Act. This includes the identification of weaknesses and strengths from a risk mitigation perspective.

3.2 Risk-based approach

In line with the Regulators' Compliance Code the Information Commissioner will adopt a risk-based, proportionate and targeted approach to audit and assessment activity.

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

- Business intelligence such as news items;
- data controller's annual statements on control;
- data controller's 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.

3.3 Engagement

The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach. For data controllers, included as part of the programme, the standard approach will be to seek their consent in line with section 51(7) of the Act.

Data controllers will be informed in writing of the Information Commissioner's intention to conduct an audit. This letter will explain the audit process, the basis on which they have been selected and a broad outline of the intended scope and the projected dates of the various audit activities.

Where there is agreement in principle to an audit the Information Commissioner will work closely with the data controller in advance of any on site audit activity. This will enable the scope to be further defined and the potential participants and a timetable 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 Appendix 2) before the 'consensual audit' starts. The letter will define the scope of the assessment and the audit objectives, both of which are primarily based on compliance with the eight data protection principles in the Act.

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

If there is to be a public announcement about a forthcoming audit, the Information Commissioner will ensure that there is effective co-ordination of this with the data controller.

3.4 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 '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 Act,

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 findings of the Audit 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 findings may also be provided during the course of the audit.

4. Assessment Notices

4.1 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 high probability that personal data is not being processed in compliance with the Act with a significant likelihood of damage and 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 risk 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 'self reported' breaches.
- 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 documentation 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 behalf of data controllers which highlight problems in 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.

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 of any likely damage or distress caused by non compliance.

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.

Details of Assessment Notices will be published on the Information Commissioner's website.

4.2 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 any specific requirements for the particular assessment such as which premises are to be entered or equipment to be inspected, and when, and of their rights of appeal under section 48 of the Act. Any appeal must be made to the Tribunals Service within 28 days of the date on which the assessment notice was served.
- The notices will set out the scope of the assessment which could be focused on the application of specific principles or business functions or on governance and control considerations.
- 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 timing of any assessment notice related activities 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 of is a high probability of significant non-compliance with the Act with serious associated risks to individual privacy.

4.3 The cancellation of notices

The Information Commissioner may cancel an assessment notice if a data controller satisfactorily explains why the assessment should not occur in the circumstances or where there is a legitimate request to postpone it.

Where a request is made for a deferment 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 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.

5. Compulsory Audits

The conduct of 'compulsory audits' will largely correspond to that of 'consensual audits' undertaken by the Information Commissioner as detailed in section 3. A schematic representation of both processes is provided in Appendix 1.

The access requirements specified in the assessment notice will enable the Information Commissioner to review, within a prescribed scope, the data controller's data protection governance framework and personal data handling practices.

5.1 Documents and information

For the purpose of compulsory audits access will be required to 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	Memorandum 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.

As required by section 41B (3) of the Act access will not be requested to information which is subject to legal privilege, which is classified as 'Top Secret' or if it has equivalent commercial sensitivity.

Access to information classified as restricted or above, with the exception of the previous paragraph 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.

5.2 Inspections and examinations

Inspections and examinations are key review elements of the audit. They are done to identify objective evidence about how policies and procedures have been implemented and how effectively they 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:

- stores, organises, adapts or alters information (eg 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 which measure how a data controller meets his 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.

5.3 Interviews

Interviews will comprise of 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 (eg 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 eg managers, operational

staff etc will be discussed and agreed. Individuals will 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.

Every effort will be taken to restrict interviews to staff identified within the agreed schedule but where it is identified 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 would not preclude confirmatory conversation with a consenting third party; for example where the third party was in close proximity to a desk side discussions.

Interviews are to help in assessing compliance. They do not form part of, or provide information for, any disciplinary investigation.

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

5.4 Compulsory audit reporting

An assessment 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 develop assurance assessments, 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:

- an executive summary;
- 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 whether compliance with the Act is unlikely.

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 subsequently 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 to take to comply with the data protection principles. In line with the principles of better regulation the recommendations will be risk rated to identify those needing immediate or urgent action.

A draft report will initially be presented to the data controller to enable them to comment on the factual accuracy of the report and to highlight any information pertinent to the report 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 attempt to address any issues identified by the data controller's comments and update the audit report as appropriate. The report will include the data controller's any 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 defined timescales then the Information Commissioner will issue the report as a final report and circulate the report to the Chief Executive Officer / Accounting Officer.

5.5 Report publication

Compulsory audit reports will be published for a year on the Information Commissioner's website. They 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 take into account any opinions from the data controller about the suitability for publication of any element of the report.

Requests made for copies of audit reports 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.

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 Assessment

The Information Commissioner does not intend that 'consensual' and 'compulsory' audits will 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 identify whether it is his intention to follow up on any data controller responses to his recommendations. Follow up may be by way of written assurances of actions taken from the data controller or a further audit.

As stated in the Information Commissioner's published guidance on the issuing of monetary penalties, the Information Commissioner will not impose a monetary penalty on a data controller where a contravention was discovered in the course of carrying out an audit.

However, he 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 had been identified.

The Information Commissioner must reserve the right to use any of his powers in the case of any identified major non-compliance where the data controller refuses to address a recommendation within an acceptable timescale.

7. Designation of data controllers

Section 41B (2) of the Act prescribes which data controllers may be served with assessment notices including 'a person of a description designated by an order of the Secretary of State'.

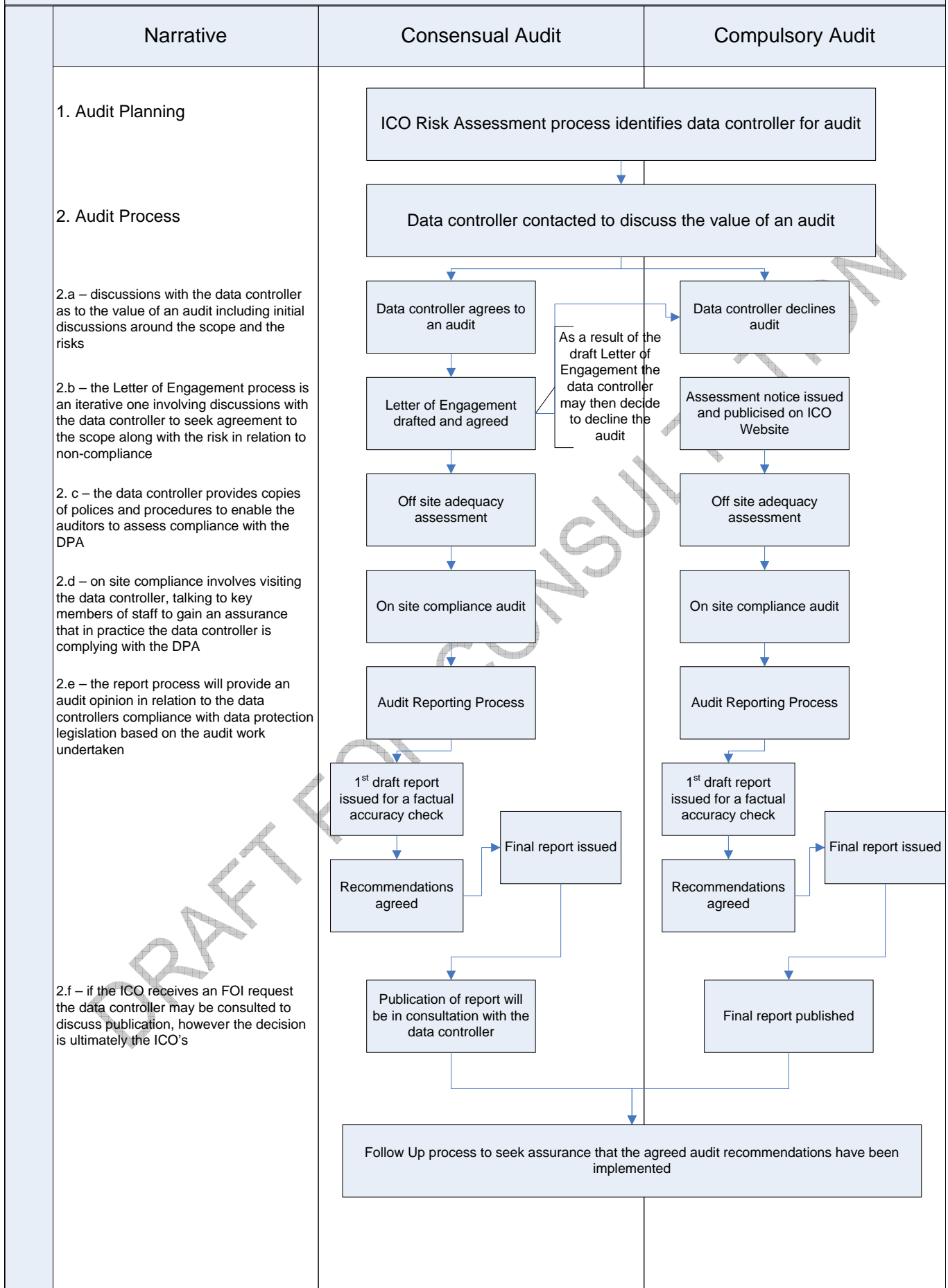
The Information Commissioner's recommendations will present a risk-based analysis of data controllers likely to be covered by the 'description' highlighting the nature and associated history of data protection issues and the potential for damage and distress to a significant number of individuals. Evidence of the unwillingness of data controllers to provide consent to audits related to the identified issues may also be presented.

In making any such recommendation the Information Commissioner will endeavour to ensure that 'descriptions' are appropriately specific.

The Information Commissioner may also make submissions of a similar nature in respect of extending the power to serve assessment notices on groups of public authorities.

8. Publication of the Code

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





Appendix 2
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 taking 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 DPA compliance.
 - 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 line with 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 the areas identified under scope but in particular the overriding risk relates to the damage to both individuals and the organisation if they fail to comply with the data protection legislation)

- 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 DPA 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 Data Protection Act
- d. A failure to appropriately control and secure manual personal data both within and outside the 'data controllers' 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 Data Protection Act.
- e. A failure to ensure Subject Access Requests are dealt with appropriately raises the risk that individual's rights to information may be compromised resulting in distress to the individual and non-compliance with the Data Protection 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.

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.

8.2 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.

8.3 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.

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

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

10. Contacts

- 10.1 Key Contact(s) within the organisation (As agreed)
- 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 Data Protection 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: