Part 1: Introduction

Foreword

A significant feature of the Data Protection Act 1998 is a provision that gives me powers to assess the processing of personal data for the following of good practice, at the invitation of a data controller. I also enjoy inspection and monitoring powers as part of my functions as the United Kingdom's designated national supervisory body under the Europol and Customs Information System Conventions.

To assist me in undertaking these functions, I commissioned the development of a data protection compliance audit methodology. The methodology consists of guidance on conducting a compliance audit and a series of checklists aimed at focussing in on the level of compliance by a data controller. I have made this manual generally available to aid data controllers who wish to undertake or commission their own data protection compliance audits. The manual contains basic auditing guidance to help ensure even small organisations with limited auditing experience can also attempt compliance auditing.

The manual is necessarily written at a high level and is not intended as a certification tool, guaranteeing compliance with the Data Protection Act. Its use serves to identify possible areas of non-compliance requiring attention by a data controller. Although use of the manual has been piloted, there is no substitute for experience of using it in practice and I look forward to hearing the reactions of those who do use it. I expect that, as we gain experience of its use, the checklist questions will be refined and may be expanded to cover issues specific to a particular sector. It is also my intention to look at the possibility of producing a less lengthy document aimed at smaller organisations without the resources to embark on a detailed compliance audit.

Ensuring compliance with the data protection standards is not simply an issue of operating within the law; it is also about the effective handling of personal information and respecting the interests of individual data subjects. I hope that this manual assists data controllers in addressing these important objectives.

Elizabeth France

Information Commissioner

Part 1: Introduction

This manual has been produced by the Information Commissioner to assist with data protection compliance auditing. It has been produced to help the Commissioner undertake her functions under section 51(7) of the Data Protection Act 1998 and as the United Kingdom's designated national supervisory body under the Europol Convention and the Customs Information System Convention and Regulation.

The manual contains a methodology for conducting data protection compliance audits together with a series of checklists aimed at testing compliance with each of the Acts main provisions. Rather than simply being tailored to the Commissioners specific needs, it has been written in such a way that any data controller can use it to help judge their own data protection compliance. Similarly, it may also be used by other organisations offering such services to data controllers. Given that potential users may have different levels of existing audit expertise, the manual also includes general guidance on compliance auditing.

Although use of the manual should help data controllers to focus on their own compliance with the Data Protection Act 1998, its use can never be a comprehensive guarantee of compliance as the manual is necessarily written at a general level for a diverse audience. It is expected that the checklist questions may develop over time as experience is gained in using these in practical situations. Given that the checklists are aimed at assessing compliance with the main elements of the Act, there is also scope for the development further sector specific checklists such as in connection with The Telecommunications (Data Protection and Privacy) Regulations 1999. The Commissioner will make any such updates available as and when they are produced.

The manual is divided into five main parts. In addition to this introduction, these deal with; the audit method, the audit process, general guidance on auditing and a series of annexes providing essential documents such as checklists containing compliance questions for each of the Acts main features and other pro forma documents.

1. Aims of Data Protection Compliance Audits

Many organisations will be familiar with existing audit methodologies used to assess compliance in areas such as Finance, Data Security, Health and Safety, Environment and Quality Assurance. The aims of Data Protection Compliance Audits go beyond the basic requirements of say Data Security and address wider aspects of data protection including:

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- Quality Assurance – ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- Retention – appropriate weeding and deletion of information.
- Documentation on authorised use of systems, e.g. codes of practice, guidelines etc.
- Compliance with individual's rights, such as subject access.
- Compliance with the data protection legislation in the context of other pieces of legislation such as the Human Rights Act.

2. Why Should Organisations Audit?

There are many sophisticated management tools available to organisations to help them undertake activities like Business Process Re-engineering, Continuous Performance Improvement, Balanced Scorecards and Business Excellence Modelling. One thing that all of these activities have in common is the requirement to conduct some sort of initial assessment or audit to establish a starting position or "baseline". This baseline information is then used as a reference against which improvements in performance over time can be measured.

As far as data protection is concerned, the key reasons for carrying out audit activities are:

- To assess the level of compliance with the Data Protection Act 1998
- To assess the level of compliance with the organisation's own data protection system
- To identify potential gaps and weaknesses in the data protection system
- To provide information for data protection system review

3. Audit Objectives

When carrying out a Data Protection Audit in any area of an organisation the Auditor has three clear objectives:

- To verify that there is a formal (i.e. documented and up-to-date) data protection system **in place** in the area
- To verify that all the staff in the area involved in data protection:
  - Are **aware** of the existence of the data protection system
  - **Understand** the data protection system
  - **Use** the data protection system
- To verify that the data protection system in the area actually **works** and is **effective**

4. What is an Audit?

For the purposes of the Manual we will define a Data Protection Audit as:

> *"A systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organisation's data protection policies and procedures, and whether this processing meets the requirements of the Data Protection Act 1998".*

The key points about Data Protection Audits that can be extracted from this definition are that:

- They involve a **systematic approach**
- They are carried out, where possible, by **independent** auditors who ideally have received relevant training
- They are conducted in accordance with a **documented audit procedure**
- Their outcome is a **documented Audit Report**

It is recognised that the smaller organisations may have resource limitations making it difficult to find fully independent auditors or to provide comprehensive training. Further information on this topic can be found in section 1.3 of Part 3.

5. Audit Categories

It is important to realise that there are many different categories of audits in common use today within the various branches of auditing. For Data Protection auditing, however, there are only three main categories of audits that we need to consider:

Description	Audit Category	Conducted by
First party	Internal	By the organisation on itself
Second party	Supplier	By the organisation on a supplier or sub-contractor
Third party	External	By the IC, its sub-contractors, or an independent consultant on the organisation

These three categories of audits are described below:

5.1 First Party Audits

First Party, or Internal Audits are those where an organisation carries out audits on itself. As we have suggested earlier they can be a very effective management tool, which can help organisations adopt a proactive and best practice approach to data protection. By establishing a regular schedule of internal audits and training staff to carry them out organisations will develop confidence in their own systems based on objective evidence. The ongoing process of auditing and being audited will also increase the general level of data protection awareness among all the staff.

5.2 Second Party Audits

Second Party Audits are commonly known as Supplier Audits because they are used where an organisation has to assure itself of the ability of a potential or existing supplier or sub-contractor to meet the requirements of the Data Protection Act.

Today there is a tendency for organisations to outsource more and more of their data processing activities. Therefore Supplier Audits are becoming increasingly important as part of the process for making the initial selection of a data processor, and then for monitoring their ongoing performance.

It should be noted that the organisation need not undertake a Supplier Audit itself if the supplier can provide evidence of having successfully passed a Data Protection Audit, provided it was conducted by a reputable and independent third party Assessment Body.

5.3 Third Party Audits

Third Party Audits involve an independent outside body coming in to the organisation to conduct an audit. For Third Party Data Protection Audits it is possible to identify two different sub-classifications:

5.3.1 Information Commissioner Investigations (Section 51)

This relates to an investigation the Commissioner may carry out under her statutory audit powers of Section 51(7) of the Data Protection Act 1998 which states:

"The Commissioner may, with the consent of the Data Controller, assess any processing of personal data for the following of good practice".

In circumstances where a Data Controller may invite the Commissioner to conduct a consensual audit of this nature, she may:

- Carry out the assessment with her own staff using the audit methodology described in this manual.
- Contract out the assessment to a third party who will also use the audit methodology described in this manual.

5.3.2 Third Party Assessments

This situation occurs when a Data Controller believes that it will be beneficial to have an independent external assessment of the effectiveness of their data protection systems. To facilitate this, the Data Controller may sub-contract the assessment to a third party (such as an audit firm) and request that they use the audit methodology described in this manual.

It is also possible that the Data Controller might want the data protection system to be assessed as part of a wider programme involving audits of areas such as Data Security, Health and Safety or Quality Management. Many organisations are now finding it more cost effective to conduct integrated audits in this way. This has already been recognised within the international auditing community by initiatives such as the new ISO 19011 provisional standard for joint auditing of Environmental Management (ISO 14001) and Quality Management (ISO 9001) Systems.

6. Audit Benefits

The previous sections have shown that organisations that adopt data protection auditing as a management tool can expect to achieve a number of benefits.

6.1 Basic Benefits from Auditing

The basic benefits that should be achieved by organisations implementing data protection audits include:

- Facilitates compliance with the Data Protection Act 1998.
- Measures and helps improve compliance with the organisation's data protection system.
- Increases the level of data protection awareness among management and staff.
- Provides information for data protection system review.
- Improves customer satisfaction by reducing the likelihood of errors leading to a complaint.

6.2 Additional Benefits from the Information Commissioner's Methodology

Furthermore, by adopting the audit methodology described in this manual, organisations can expect to achieve additional benefits, including the ability to:

- Use an existing "model of audit best practice" rather than having to re-invent the wheel.
- Use the same methodology as that used by the Commissioner.
- Quickly establish an internal audit programme by adopting and adapting the audit pro formas and checklists that the Commissioner has put into the public domain.