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.

Part 2: The Audit Method

Illustrations

Part 2: The Audit Method

The purpose of this part of the Audit Manual is to explain the background to the two-part audit methodology that is used by the Commissioner as the basis for conducting assessments of how organisations handle the processing of personal data. We will also describe the options available to the Auditor when conducting the different categories of Data Protection Audits and outline the key concepts behind the methodology.

1. Audit Categories

Section 5 of Part 1 has already discussed the concepts of First, Second and Third Party Audits. The best way to understand the differences between them is by reference to Figure 2.1 below:

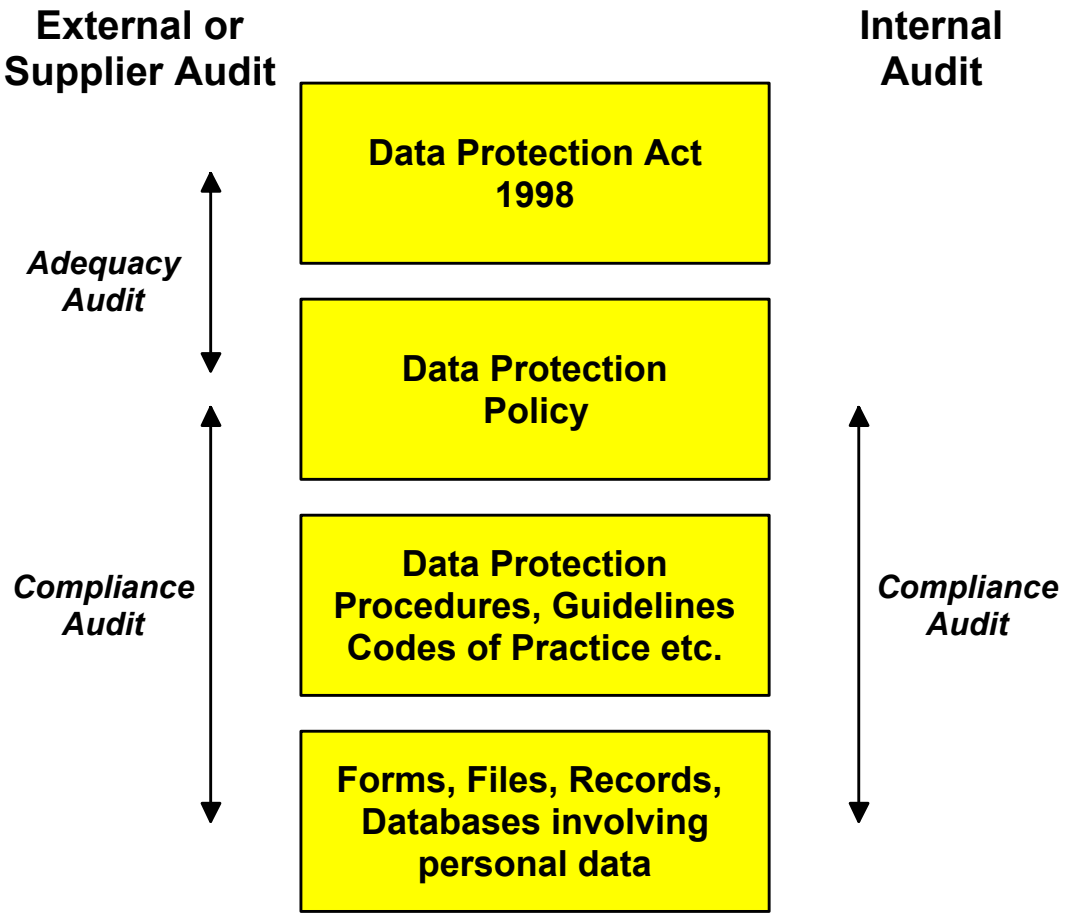


Fig. 2.1: The Three Audit Categories

It can be seen from Figure 2.1 that ideally, External and Supplier Audits (i.e. Third and Second Party) are conducted in two parts, namely an Adequacy Audit followed by a Compliance Audit. Internal Audits (i.e. First Party) are conducted as a single Compliance Audit. It is important to realise that Adequacy and Compliance Audits fulfil different purposes in this methodology.

1.1 Purpose of Adequacy Audits

The purpose of the Adequacy Audit is to check that any documented Policies, Codes of Practice, Guidelines and Procedures meet the requirements of the Data Protection Act 1998. This part of the audit is performed first and is a desktop exercise that can usually be conducted off-site.

It is possible, of course, for an Adequacy Audit to be conducted by Internal Auditors provided they have the necessary specialist understanding of the requirements of the Data Protection Act.

1.2 Purpose of Compliance Audits

The purpose of the Compliance Audit is to check that the organisation is in fact operating in accordance with its documented Policies, Codes of Practice, Guidelines and Procedures. It is the most important part of an audit and has to be conducted on-site.

An obvious question raised by Figure 2.1 is why an Internal Audit only involves a Compliance Audit? The reasons for this are that the following assumptions are made:

- It is more effective carrying out scheduled Internal Audits on data protection systems that have been formally documented and are fully operational.
- The data protection system will in theory meet the requirements of the Data Protection Act 1998 because it should have been designed specifically with this objective.
- If the data protection system is mature it may well have been subjected to an earlier Adequacy Audit by independent third parties as part of the implementation process.

Therefore, it is normal practice for Internal Audits not to include an Adequacy Audit. **There is of course no reason why organisations cannot conduct Adequacy Audits as part of their Internal Audit programmes should they so wish, and in fact this might prove quite beneficial for new systems where outside help has not been involved.**

1.3 Audit Evidence

It should be apparent from the previous sections that Internal and External audits are looking for evidence concerning different aspects of a data protection system. These different aspects relate back to the original Audit Objectives detailed in Section 3 of Part 1 and are summarised in the table below:

Audit Objective	Evidence Sought	Adequacy Audit	Compliance Audit
The system **EXISTS** and is **ADEQUATE**	Documentation, e.g. Data Protection Policy, Procedures etc.	Yes	Yes (assumed)
The system is **USED**	Records of Subject Access Requests, Complaints etc.	No	Yes
The system **WORKS**	Corrective Actions, System updates and improvements	No	Yes

The above table should help to make the distinction between Adequacy and Compliance Audits even clearer, i.e.

- The Adequacy Audit's prime concern is that there is a documented data protection system that adequately addresses all aspects of the Data Protection Act.
- The Compliance Audit is concerned with how the data protection system is being used and how effective it is.

2. Adequacy Audit Outcomes

It is very important for Second and Third Party Audits that the Adequacy Audit is conducted first as the results of the Adequacy Audit will determine what happens next in the process. The two possible outcomes of an Adequacy Audit are:

2.1 Satisfactory Adequacy Audit

If the Adequacy Audit indicates that the organisation has a documented data protection system in place with perhaps only a small number of gaps or deficiencies, the Auditor can continue with a Compliance Audit as described in section 3.

2.2 Unsatisfactory Adequacy Audit

The Adequacy Audit may indicate that the organisation has very little data protection documentation in place with inadequate procedures and major gaps in areas such as data protection awareness training. If an Auditor uncovered such major deficiencies at this preliminary stage, they must make a policy decision as how to proceed. In these circumstances there are three options:

- The organisation may still wish to go ahead with a Compliance Audit to help formulate potential solutions to address the key gaps and weaknesses already identified in its systems
- The Auditor can inform the organisation that there is little point in conducting the Compliance Audit until the major deficiencies have been addressed.
- The Auditor can refer the organisation to the Commissioner or others providing data protection advice and guidance in order to rectify the deficiencies in the data protection system.

3. Compliance Audit

There are 2 basic methodologies that are commonly used for conducting Compliance Audits and these can either be used separately or in combination on each audit.

3.1 Functional or Vertical Audit

This type of audit involves checking all aspects of the data protection system within a particular area, function or department. A Functional Audit concentrates on processes, procedures and records restricted to the department itself and does not cross inter-departmental boundaries. It is recommended that Auditors question data protection staff during Functional Audits because they should be most familiar with how departmental systems implement the organisation's overall data protection policies.

A typical example of when it would be appropriate to conduct a Functional Audit would be where it was required to assess the compliance of a Human Resources department. In this case most of the procedures, personnel files etc. associated with the Human Resources function are likely to reside wholly within the department itself. The Functional Audit could then restrict itself to checking all the activities involving the gathering and processing of personal data within the department.

The way that such a Functional Audit would be undertaken is illustrated graphically in Figure 2.2 which represents the structure of a typical organisation as being divided into separate, vertical, functional departments. It shows how the Functional Audit would only affect the Human Resources department but would also have to examine the Data Protection Policy, Organisational Resources and Records that directly relate to the Human Resources function.

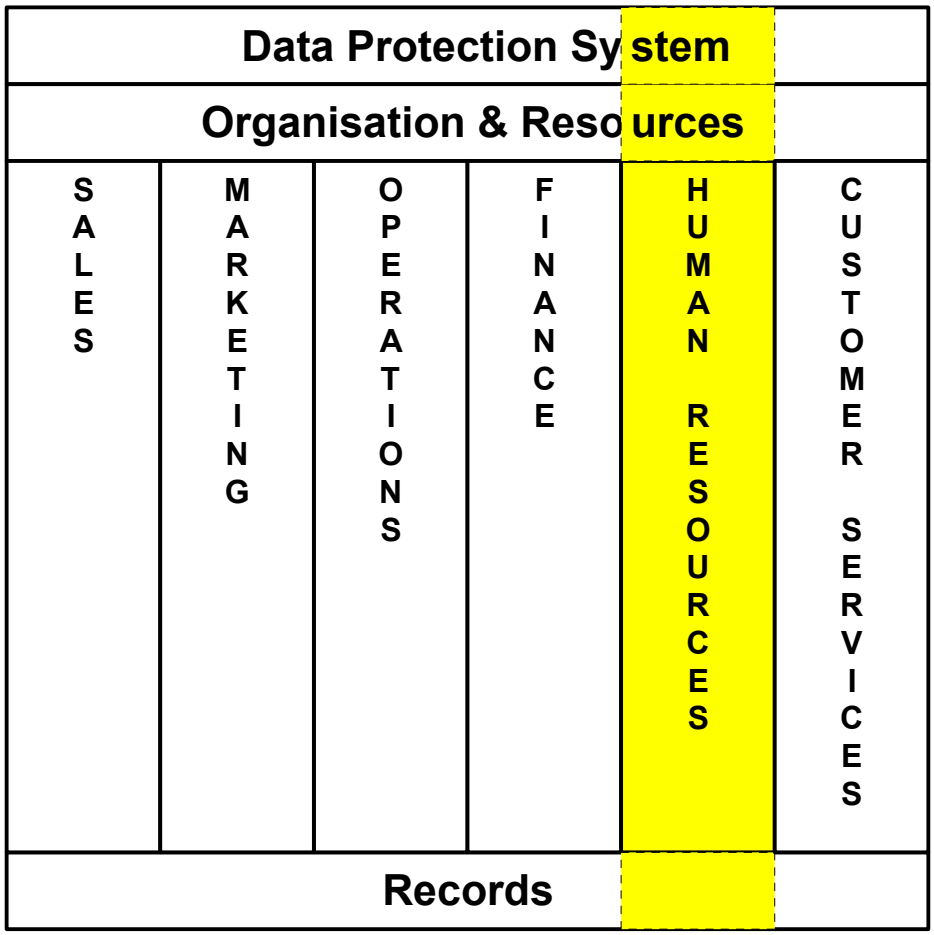


Fig. 2.2: Functional or Vertical Audit

3.2 Process or Horizontal Audit

This type of audit involves tracking a particular process from one end to the other. A Process Audit will cross a number of interfaces between areas, functions or departments. It is the key to understanding how an organisation functions and is best conducted with front-line, operational staff.

A typical example of when it would be appropriate to conduct a Process Audit would be where it was required to assess the processing of Data Subject Access Requests. In this case the processing of these requests is likely to involve the co-operation of a number of different departments within the organisation. The Process Audit would follow the progress of the Subject Access Request as it was processed by the various departments and staff involved. Another example could be the process for approving a new application form that involved the collection of personal data. The form could typically originate with the Marketing Department, but might need to be checked by Sales, Operations, Finance, Legal and IT and should certainly require some form of data protection sign off.

The way that such a Process Audit would be undertaken is illustrated graphically in Figure 2.3, which shows how processes like Subject Access Requests may cut horizontally across many different inter-departmental boundaries. Section 3.3.2 of Part 3 describes how the Auditor has the choice of either starting at the beginning of a process and tracing forward, or starting at the end and tracing backwards.

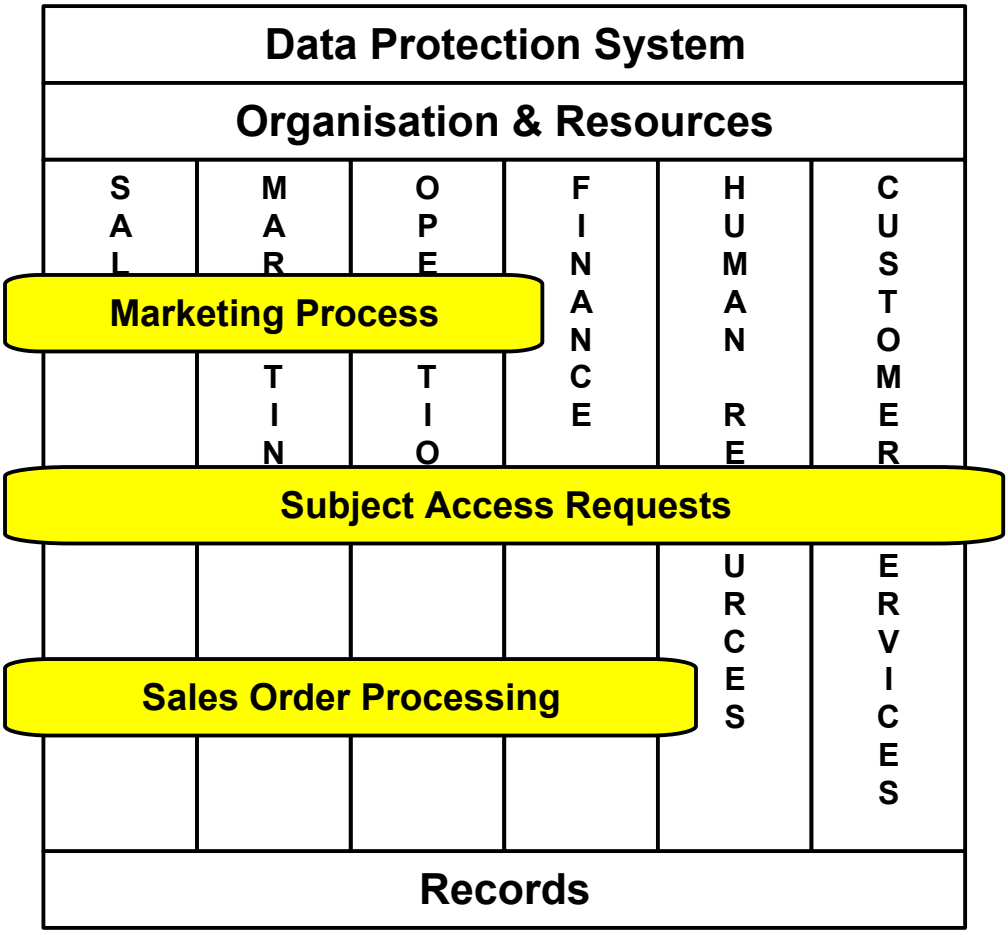


Fig. 2.3: Process or Horizontal Audit

3.3 Interactions with Staff

It is very important to realise that no matter how well thought out and documented an organisation's data protection procedures might be, they still rely on people for their operation. It is impossible therefore, for an Auditor to do a thorough job unless they speak to the staff involved in the activities being audited, and this dialogue should occur in two distinct ways.

3.3.1 Staff Questioning

Whether conducting Functional or Process Audits it will be necessary to ask staff to answer a series of questions based on the Checklists provided in Annexes F, G, H and J. The purpose of this questioning is to obtain sufficient evidence to decide whether what is actually taking place complies with what the data protection system says should occur in practice. In this situation the Auditor is effectively behaving like an interviewer. It is therefore important that a good rapport is established with the interviewee so that the required information can be obtained as quickly as possible. The Auditor will also need to have a good questioning techniques, and tips about this and the other human aspects of auditing will be found in Part 4.

3.3.2 Staff Awareness Interviews

As well as speaking to members of staff to obtain specific items of information, Auditors need to assess the general level of staff awareness of data protection issues and their commitment to protecting the privacy of personal data. Perhaps the best way of assessing staff awareness during an audit is by means of either:

- One-to-one interviews
- Focus groups

- depending upon the number of staff in the organisation and the amount of time available. The Audit Manual provides guidance for conducting these sessions in Section 3.3 of Part 3, and also supplies a series of suitable interview questions in Annex D.4.

In circumstances where it is just not possible to conduct staff interviews then Auditors may wish to prepare Data Protection Awareness Questionnaires based on the material supplied in Annex D.4. However, this approach should only be used as a last resort as it is inferior to direct face-to-face contact.

Part 3: The Audit Process

Part 3: The Audit Process

Illustrations

Part 3: The Audit Process

A Data Protection Audit is a process involving a number of separate activities or phases that may occur over an extended period of time. To manage this process effectively it is necessary to understand the five phases that comprise a typical audit:

- **Audit Planning**
- **Audit Preparation**
- **Conduct of the Compliance Audit**
- **Compliance Audit Reporting**
- **Audit Follow-up**

This part of the Audit Manual describes these five phases of the "Audit Lifecycle" in a chronological step-by-step fashion. Wherever reference is made to a pro-forma, examples have been provided in the appropriate annex. The Audit Lifecycle illustrated in Figure 3.1 below:

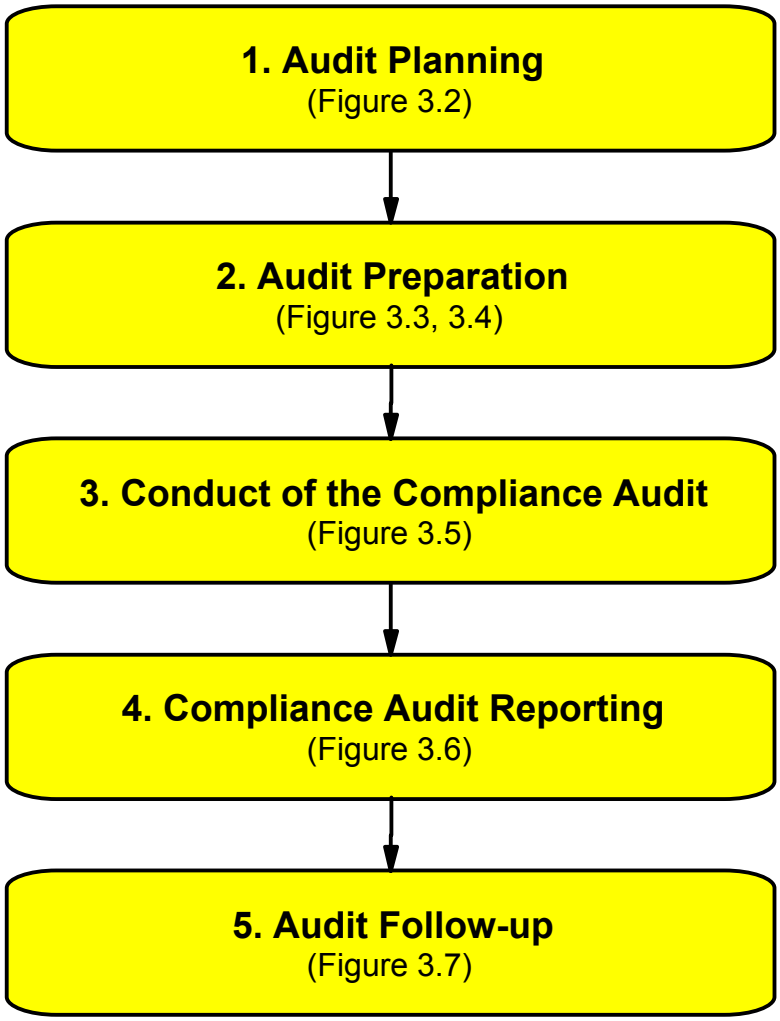


Fig. 3.1: The Data Protection Audit Lifecycle

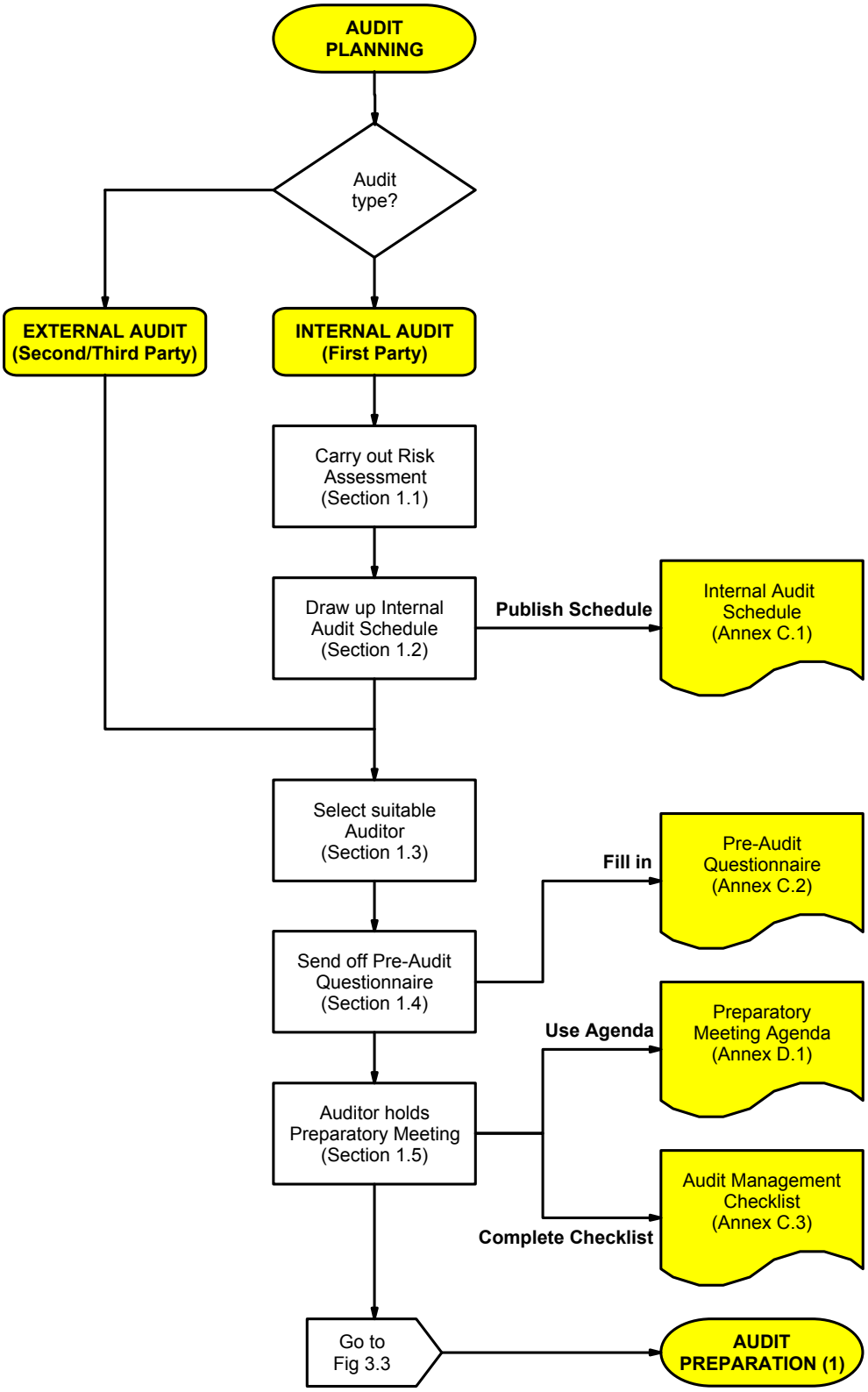


Fig. 3.2: Audit Planning

1. Audit Planning

The more work that is put in to the planning and preparation of an audit, the smoother the conduct of the audit will be on the day. Typically, about 25% of the total effort involved in the audit should be devoted to careful work during these early stages. If you are relatively new to auditing then you may need to allow even more time to ensure a smooth transition to the later stages of the audit.

The five key aspects of Audit Planning are covered in the sections that follow and are also illustrated in flow chart form in Figure 3.2. Sections 1.1 and 1.2 really apply only to those organisations that wish to set up their own internal system for conducting Data Protection Audits.

1.1 Risk Assessment

Experienced auditors will want to conduct a full risk assessment to determine which areas are to be audited and with what frequency before drawing up the Audit Schedule of section 1.2. A straightforward method for carrying this out will be found in Annex A if required.

Novice auditors or organisations that are introducing internal Data Protection Audits for the first time can adopt a much simpler practice which is to ensure that every function or area is audited within a particular timeframe such as perhaps at least once per year.

1.2 Audit Schedule

Once an organisation has decided to operate an Internal Data Protection Audit Programme, it will find that an annual Audit Schedule is an essential control mechanism. The Audit Schedule will help to ensure that the areas within the organisation that handle personal data will be audited on a planned and systematic basis. The steps involved in producing and maintaining an Audit Schedule are described in the following sections.

1.2.1 Audit Schedule Generation

An Audit Schedule is used to record which areas of the organisation should be audited and when, a pro-forma like that shown in Annex C.1 could be used for this purpose. The areas to be audited should be recorded in the first column, and the audit frequency should be entered in the second column. If required this information can be calculated as shown in Annex A, otherwise the frequency can simply be once per year. The remaining 12 columns are then used to record the dates scheduled for each audit during the year.

It is very useful to give each audit a sequential reference number for cross-referencing purposes, and this number can also be entered on the schedule after each scheduled date.

1.2.2 Audit Schedule Approval and Publication

As the Audit Schedule is such an important component of an organisation's Data Protection Compliance Programme it needs to be owned and published by Senior Management. For example, the draft schedule could be drawn up by the person responsible for Data Protection and then presented to Senior Management for approval. Once this has been obtained the Audit Schedule could be distributed to all Heads of Departments and any other staff affected.

If the organisation actually has a Data Protection Forum/Committee, or an Audit Committee, then this could play a key role in the approval process prior to the Audit Schedule being presented to Senior Management.

1.2.3 Audit Schedule Maintenance

An Audit Schedule is best produced and updated on an annual basis. However, there may be circumstances where the schedule needs to be updated before the end of the year, for example if a new department is created, or the audit frequency within a particular area needs to be changed for any reason. In these circumstances the Audit Schedule should be updated and re-distributed and all copies of the previous schedule removed. If the organisation already operates a Quality Management System like ISO 9000 then the easiest way of doing this is to control the Audit Schedule via the existing ISO 9000 Document Control process.

1.3 Selection of Auditor

The key factor to bear in mind when selecting staff to carry out Data Protection Audits is that they should be independent of the function being audited. This means that ideally the person responsible for Data Protection should not audit activities such as Subject Access Requests if they usually process these themselves. However, in small organisations it may be very difficult or even impossible to ensure total independence and so a compromise will have to be reached. In larger organisations, there should be positive benefits by having staff from one function auditing another as this might encourage the adoption of best practice.

Auditors who are required to carry out Data Protection assessments will need to meet certain minimum criteria in a number of areas. The international auditing standard ISO 10011-2 can serve as a very useful starting point to help organisations define these minimum criteria, and some recommendations are made for both Internal and External Auditors.

1.3.1 Skills

All Data Protection Auditors should be competent at expressing concepts and ideas clearly and fluently both orally and in writing.

1.3.2 Training in Auditing

Ideally, every Auditor should be given adequate training before conducting any audits.

a) External and Supplier Auditors

When choosing an External or Supplier Auditor, organisations should check that they have been trained to a level sufficient to ensure competence in the skills required for both conducting and managing audits. The core areas covered by this training should include:

- Knowledge and understanding of Data Protection issues in general and the 1998 Act in particular.
- Familiarity with the assessment techniques of examining, questioning, evaluating and reporting.
- Additional skills for managing an audit, such as planning, organising, communicating and directing.

b) Internal Auditors

Internal Auditors, particularly those in smaller organisations are unlikely to have received training to the level described above. For this reason Part 4 of this Manual and the pro formas and checklists in the Annex are intended to provide novice auditors with sufficient guidance to conduct basic Data Protection audits without further training.

1.3.3 Experience of Data Protection Law and Practice

Internal and External/Supplier Auditors may have very different levels of experience of Data Protection Law and Practice.

a) External and Supplier Auditors

When choosing an External or Supplier Auditor it is recommended that organisations look for Auditors who have demonstrable experience in Data Protection related activities.

b) Internal Auditors

Smaller organisations will probably have great difficulty in finding staff with much experience of Data Protection Law and Practice, so again the best compromise will have to be reached. Larger organisations may find that only the person(s) responsible for Data Protection has the relevant experience, but this should not preclude other staff from auditing for the reasons stated in 1.3.2 b).

1.3.4 Personal Attributes

Both Internal and External/Supplier Data Protection Auditors will require the following personal attributes if they are to carry out their tasks successfully:

- To be open-minded and mature in approach
- To possess sound judgement, analytical skills and tenacity
- To be objective
- To have the ability to perceive situations in a realistic way
- To be able to understand complex operations from a broad perspective
- To be able to understand the role of individual units within the overall organisation

1.4 Pre-Audit Questionnaire

Auditors should try and find out as much background information as possible about the organisation before conducting a Preparatory Meeting/Visit of the type outlined in section 1.5. To achieve this, it is recommended that a Questionnaire be sent to the organisation who is requested to complete it and return it to the Auditor prior to the visit. This Questionnaire should elicit basic name and address type information as well as allow the organisation to describe the scope of its data protection activities in simple terms. The Pre-Audit Questionnaire of Annex C.2 has been designed with these objectives in mind.

Where Auditors are dealing with large organisations they may find it necessary to complete one Questionnaire for each department or area. It is also a very good idea to ask for an organisational chart or “organogram” at this stage as it may clarify the structures described in the Questionnaire.

1.5 Preparatory Meeting/Visit

It is important that there is effective liaison carried out between the Data Protection Auditor and the organisation before, during and after a Data Protection Audit. The extent and manner of this liaison will vary depending upon whether the Audit is first, second or third party.

In the case of a first party or internal audit, all that is usually required is for the Auditor to arrange a visit with the person responsible for Data Protection to discuss the details of the audit using the outline agenda below. For second or third party audits the most efficient method of liaison is for the Auditor to set up a separate Preparatory Meeting/Visit with the organisation four to six weeks before the Audit.

The details that need to be discussed and confirmed at a Preparatory Meeting come under the following headings:

1.5.1 Administration

Topics to be discussed here include:

- **Contact details:** who is the key Data Protection contact within the organisation for liaison purposes before, during and after the audit?
- **Documentation:** what documentation should the organisation send in advance for the auditor(s) to conduct the Adequacy Audit?

1.5.2 The Audit

The following aspects of the Data Protection Audit itself need to be discussed and agreed at the Preparatory Meeting:

- **Scope of audit:** what departments and/or functions will be involved?
- **Audit timescales:** when does it start and what is the likely duration?
- **Personnel affected:** which staff within the organisation will be involved in the audit?
- **Meetings:** when and where will the opening and closing meetings take place and who will be present?
- **Audit Plan:** what is the likely schedule for the auditor(s) visiting the departments/functions and staff involved in the audit?
- **Reporting:** what type of written/oral feedback will the auditor(s) be presenting to the organisation, and when will it be presented?
- **Follow-up:** what are the arrangements for follow-up audits/visits to confirm corrective action has been taken where necessary?

1.5.3 Practical Arrangements

It is important to establish exactly which facilities will be required by the Auditor(s) during the Audit including:

- Access to premises
- Base room/office availability
- Working space, desks, furniture etc.
- Access to IT equipment, e.g. PCs, printers, modems etc.
- Access to telephones, photocopiers, shredders etc.

A suggested agenda for the Preparatory Meeting will be found in Annex D.1. Further guidance to novice auditors concerning the approach to adopt when conducting meetings and audits will be found in Part 4 Section 5 of this Manual.

1.6 Audit Management Checklist

When undertaking a Data Protection Audit and working through the five phases of Figure 3.1, Auditors will find that they will have to keep track of a lot of information if the audit process is to be controlled effectively. To help Auditors with this task the Audit Management Checklist of Annex C.3 has been designed to keep track of all the personnel, meetings, documents and pro formas associated with the audit. It is recommended that Auditors start filling in the Checklist at the Preparatory Meeting and then use it to monitor the process at each subsequent stage. Space has been left on page 2 of the Checklist for making notes during the Preparatory Meeting.

2. Audit Preparation

It has already been stated in the Audit Planning section that the more planning and preparation that goes into the Data Protection Audit, the more successful it will be. This of course applies equally to the Audit Preparation stage, which covers the activities undertaken by the Auditor immediately after the Preparatory Meeting up until the Audit itself.

The four key aspects of Audit Preparation are covered in the sections that follow and are also illustrated in flow chart form in Figures 3.3 and 3.4.

2.1 Adequacy Audit

Part 2 of this Audit Manual has explained that the Audit Methodology involves carrying out an initial Adequacy Audit before the Compliance Audit. The purposes of the Adequacy Audit are therefore twofold:

- To assess the extent to which the organisation's Data Protection System meets the requirements of the 1998 Data Protection Act.
- To ascertain whether it will be beneficial to conduct a subsequent Compliance Audit or whether to delay matters until the identified in the Data Protection System have been addressed.

2.1.1 Audit Timescale

The Adequacy Audit should take place after the Preparatory Meeting/Visit and at least 2 or 3 weeks before the Compliance Audit is scheduled. This is to allow the organisation time to put right any minor deficiencies in their documentation.

2.1.2 Documentation Review

The documentation to be assessed will already have been discussed and agreed at the Preparatory Meeting/Visit (see section 1.4) and provided to the Auditor. The review of this documentation should be conducted off-site to cause as little disruption as possible to the organisation. However, in some circumstances it may be necessary to carry out the review in-situ, for example if the documentation is excessively bulky, or if it is totally computer-based.

The Auditor should ensure that the documentation supplied for assessment includes:

- **Policies:** Copies of the Data Protection Policy Statement or Manual or other top-level documents that describe how Data Protection issues are dealt with by the organisation.
- **Codes of Practice:** Any industry or sector-specific Codes of Practice that regulate how the organisation operates and which cover Data Protection.
- **Guidelines:** In-house guidance or training materials the organisation has produced to increase staff awareness of Data Protection issues.
- **Procedures:** In-house procedures that provide detailed step-by-step instructions to staff on how to deal with specific Data Protection issues, e.g. Subject Access Requests.

Auditors should be aware of the possibility that an organisation may have relevant documentation that does not specifically refer to data protection, for example a patient confidentiality policy. Such documents can be valuable in judging adequacy and need to be taken in to account

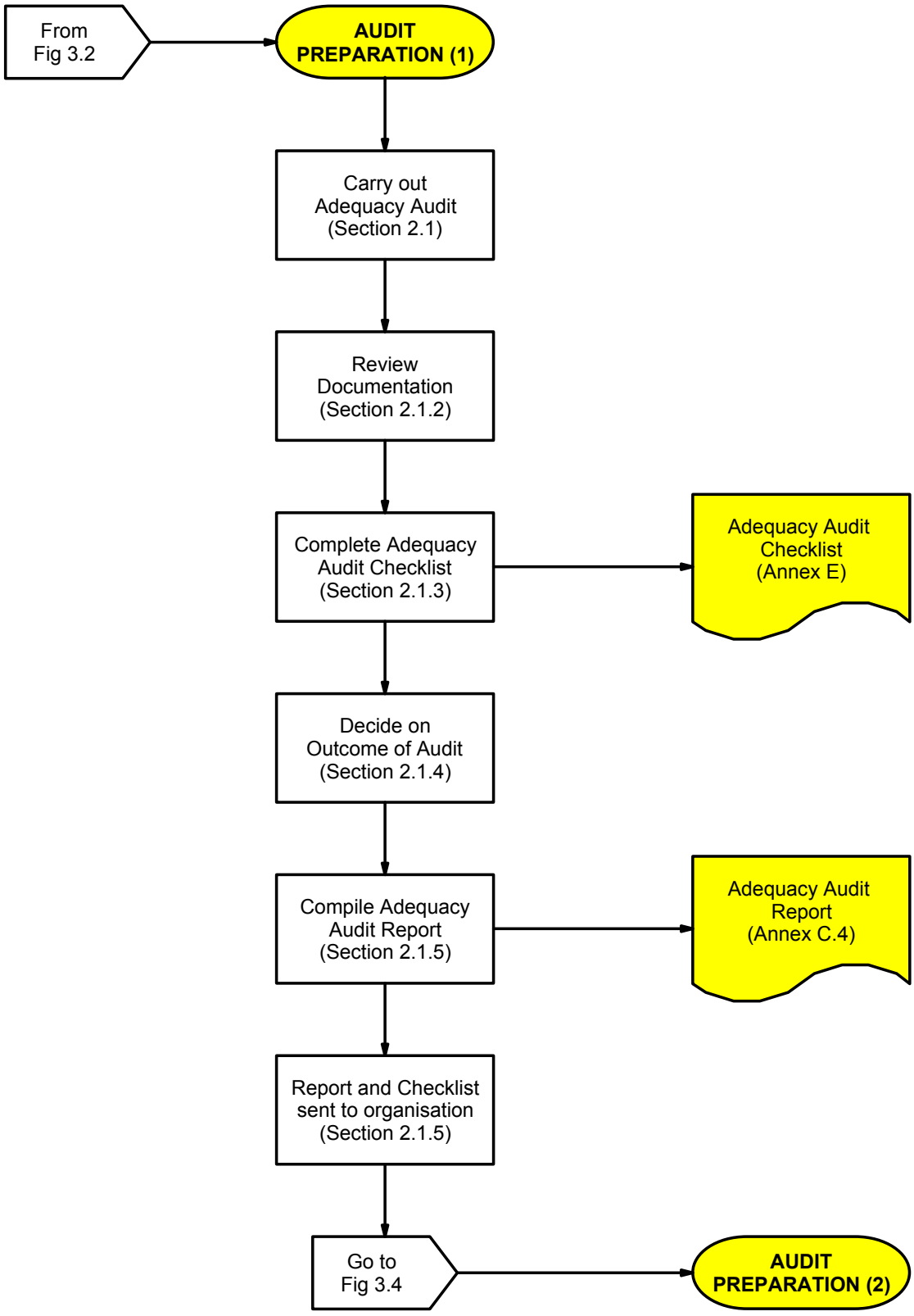


Fig. 3.3: Audit Preparation (1)

2.1.3 Adequacy Audit Methodology

The methodology used for conducting an Adequacy Audit is a much-simplified version of a Functional or Vertical Compliance Audit (see Part 3 Section 3.2.1) and involves the following steps:

- The Auditor reads carefully through all of the documentation supplied
- While reading the documentation the Auditor checks that it addresses each of the areas identified in the Adequacy Audit Checklist of Annex E. This checklist is based on the Compliance Audit Checklists of Annexes F, G and H, but only uses the main headings of each, and not the detailed questions.
- The Auditor records the corresponding reference(s) to the organisation's documentation where the answer to each question on the checklist can be found. The second column on the checklist is used for recording this reference and should include the document title, section and/or page number.
- For each question on the checklist the Auditor records to what extent the documentation addresses the issue. It should be recalled that during an Adequacy Audit the Auditor is looking for the existence of broad systems and structures to address Data Protection issues and not the fine detail.
- The final column of the Adequacy Audit Checklist is used to record this assessment using one of three categories:

Assessment	Enter
Documentation addresses issue adequately	✓
Documentation does not address issue adequately?	
No reference can be found to the issue in the documentation	×

2.1.4 Adequacy Audit Outcome

Section 1 of Part 1 has shown that the Adequacy Audit can have either a satisfactory or unsatisfactory outcome. The criteria used to make this decision are as follows:

a) Satisfactory Outcome

If the majority of assessments on the Adequacy Audit Checklist are "✓" with occasional "?" ratings the Audit will have a satisfactory outcome. In this case the organisation can proceed to the next stage of the audit process which is the on-site Compliance Audit.

b) Unsatisfactory Outcome

The types of deficiencies that will result in an unsatisfactory Adequacy Audit include:

- Failure to address any of the Parts or Schedules of the 1998 Data Protection Act or any of the 8 Data Protection Principles.
- Lack of a documented Data Protection Policy.
- Failure to identify the organisational structure, roles and responsibilities that ensure the Data Protection Policy is implemented.
- Lack of documented procedures to deal with specific Data Protection issues.

This situation will result from one or more "✗" assessments recorded against each main heading of the Adequacy Audit Checklist

In the case of an unsatisfactory outcome, the options available to the organisation are those listed in Section 1.2 of Part 1. It may still be appropriate to conduct a Compliance Audit as this may identify areas that need addressing in the Data Protection System. The Commissioner, when assessing compliance with the Act, would usually wish to examine what happens in practice before coming to any conclusions on non-compliance.

2.1.5 Adequacy Audit Reporting

The results of the documentation review are recorded in an Adequacy Audit Report. It is recommended that a pro-forma is used for this report, and a suggested layout is given in Annex C.4.

The completed Adequacy Audit Checklist is sent to the organisation together with the Adequacy Audit Report. This allows the organisation to comment on the results and rectify any minor deficiencies before the Compliance Audit takes place.

2.2 Confirmation of Audit Schedule

It is good practice for the auditor(s) to contact the key Data Protection contact within the organisation a few days before the audit is to take place in order to check that all the necessary arrangements have been made. Any minor changes to the scope of the audit and the audit plan can also be discussed and the availability of staff during the audit confirmed.

2.3 Audit Checklists

Experience from auditing Health and Safety, IT, Quality Assurance, Environmental and Financial Systems has shown that the preparation of Checklists is an essential component of any successful audit. We believe that this is equally true of Data Protection System Auditing and therefore this section will deal with the preparation and use of Checklists during a Data Protection Compliance Audit.

2.3.1 The Role of an Audit Checklist

It is possible to identify a number of important roles for Checklists before, during, and after an audit:

- They are an aid to planning and preparation before the audit
- They act as an "aide-memoir" during the audit
- They help to focus on essentials
- They help to maintain audit direction and continuity
- They are used for note taking during the audit
- They are used as the basis for reporting after the audit

2.3.2 Disadvantages of Checklists

Although Checklists are extremely useful when used properly, they can also have the following disadvantages if used incorrectly:

- They may inhibit flexibility
- There may be some degree of repetition on matters already covered
- If used by the Auditor merely as a list of questions they may:
  - Annoy the auditee due to the lack of interaction and discussion
  - Reduce the interaction and as a result cause important areas to be missed due to the lack of discussion
  - Cause compensating controls to go unnoticed

2.3.3 Functional Audit Checklists

To overcome the disadvantages listed in section 2.3.2 it is recommended that each Checklist used for a Functional Audit (see Part 2, Section 2.1) contains two types of questions:

- There are a number of standard, pre-printed questions that are used every time the system is audited.
- Space is provided throughout the checklists for a number of additional questions specific to each audit. These may either be prepared in advance by the Auditor, or should be written down during the audit as they arise.

It is also very useful to talk around the pre-printed questions during the audit to elicit additional information from the auditee. This in turn may prompt the Auditor to pose further questions which should be documented via the checklists as described above.

The Commissioner has drawn up a number of standard questions for use during Functional Audits and these are grouped into three sections:

a) Organisational and Management Issues

A set of three Audit Checklist pro formas is provided in Annex F.1 to F.3 inclusive. These checklists are used to investigate the following key organisational and management aspects of Data Protection within an organisation:

- The Data Protection System
- Documentation Issues
- Key Business Processes

b) The Eight Data Protection Principles

A set of Audit Checklist pro formas for the Eight Data Protection Principles is provided in Annexes G.1 to G.8 inclusive. The key features of these pro formas are:

- The questions relating to each Principle are grouped under a number of appropriate sub-headings that relate back to the areas of Data Protection covered by that Principle. These sub-headings are also the ones used in the Adequacy Audit Checklist of Annex E.
- After the standard questions provided under each sub-heading, space has been provided on the pro-forma for the Auditor to write their own questions specific to each audit.

c) Other Data Protection Issues

A further set of Audit Checklist pro formas has been provided in Annexes H.1 to H.3 inclusive to deal with other general aspects of Data Protection. These usually relate to the corporate level of an organisation rather than to individual departments and cover the following areas:

- Using Data Processors
- Notification
- Transitional Provisions

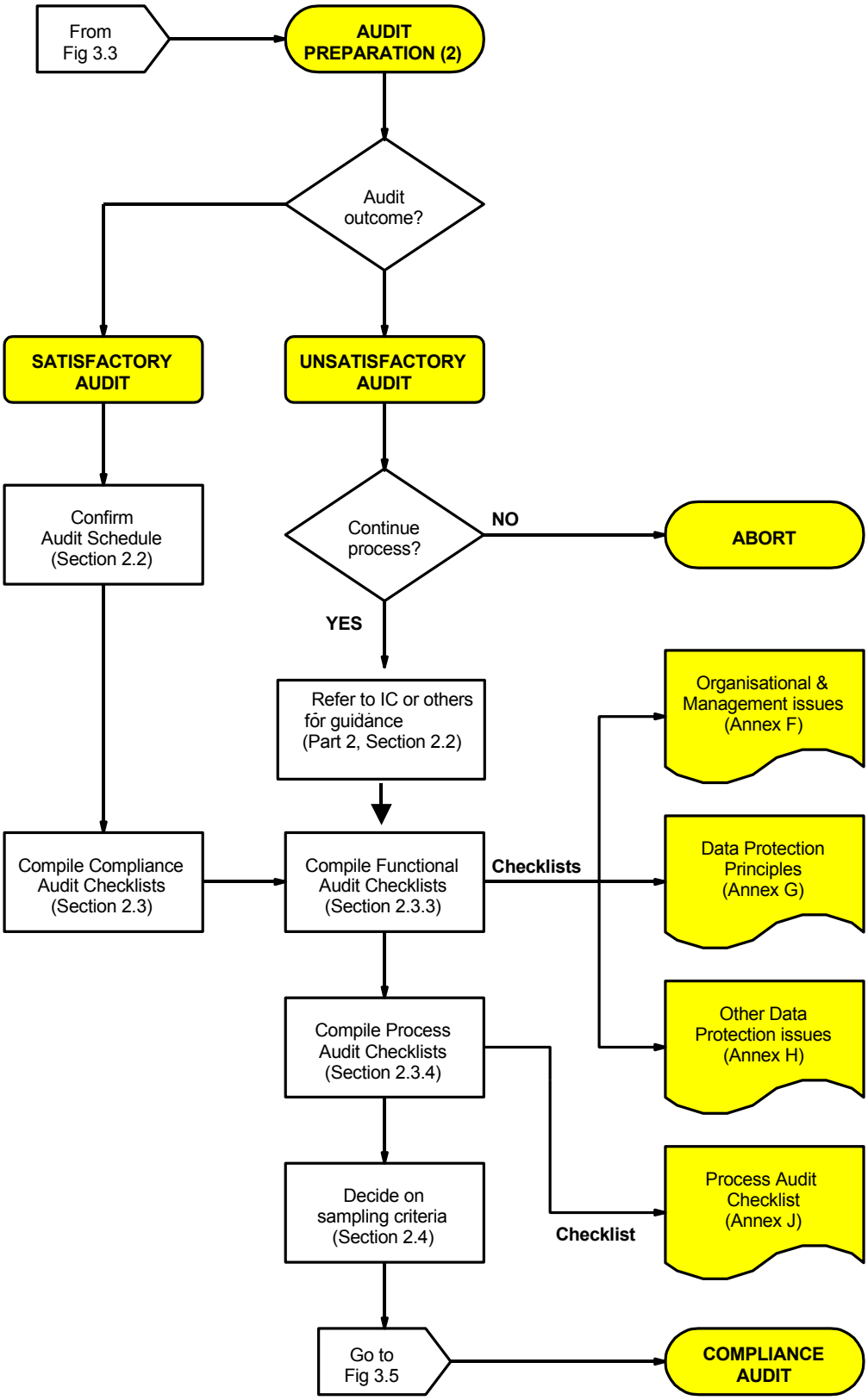


Fig. 3.4: Audit Preparation (2)

2.3.4 Process Audit Checklists

A Data Protection Audit should not only examine the Data Protection Systems operating within individual areas of an organisation, but should also track key operating processes that cross inter-departmental boundaries. Most of these operating processes will be unique to each organisation or department, and this is also true for processes that involve aspects of Data Protection such as the handling of Subject Access Requests. The role of a Process Audit is to track the operation of these processes from beginning to end to ensure that the requirements of the Data Protection Act are met at every stage.

It will be apparent from Section 2.3.3 that whereas it is possible to draw up a considerable number of checklist questions in advance for a Functional Audit, this is not the case for a Process Audit. Therefore, the Auditor will have to draw up a fresh set of Checklist questions each time a particular process is audited, and to make this easier a blank Process Audit Checklist has been provided in Annex J.

2.3.5 Checklist Preparation

When preparing checklists, auditors should remember that the fundamental purpose of each audit is:

- To collect objective evidence about the status of the Data Protection System in the organisation/department so that an informed judgement can be made about its adequacy and effectiveness.

- The Auditor must therefore take samples from the selected area and check for implementation and effectiveness of the Data Protection System in order to arrive at that informed judgement.

In effect the Checklist defines the sample so that the Auditor must make it as representative as possible within the objectives of the audit. Auditors may find it helpful to bear the following points in mind when designing their own questions to supplement the Checklists of Annexes F, G and H:

- Where the Data Protection System is thoroughly documented checklist questions may be quite specific, but in the absence of documentation questions may need to be of a broader nature.

- Experienced Auditors may be able to just write down key words whereas less experienced Auditors will feel more confident writing out questions in full.

- Think in terms of “what to look at” and “what to look for” when preparing checklist questions.

- To ensure the audit sample is representative first focus on the main function of the department or area.

- Do not neglect more peripheral activities completely as these may not be quite as well controlled and hence are more likely to be the cause of a breach.

- It is also a good idea to examine what happens when systems are under pressure rather than functioning as normal. For example, what happens:

    - When a lot of staff are off sick or on holiday?
    - When there are major changes in the workforce?
    - At the end of the month or the financial year?
    - When the computer system breaks down?
    - When work levels are abnormally high? For example, in an Insurance Company when there is a flood of insurance claims after a major storm.

2.4 Sampling Criteria

In situations where it is necessary to sample records from manual or computer files guidance on choosing the size of the sample can be found in Annex B.

2.5 Audit Plan

At this stage of the audit preparation process the Auditor should be in a position to draw up an Audit Plan showing the timetable of activities during the Compliance Audit and specifying exactly who will do what, when and where. It is recommended that a pro-forma is used for this purpose and a typical Audit Plan is provided in Annex C.5.

Auditors will appreciate that there is a lot of work to do over a short period during an audit and it is important that their time is used as efficiently as possible. The utilisation of their time can be maximised by giving careful thought to the sequence in which the audit is conducted. Some points of good practice to bear in mind when drawing up the Audit Plan include:

- Start off with a Functional Audit working through the Checklists of Annexes F, G and H with the Data Protection Manager/Officer or other senior staff member. This will allow the Auditor to build up a “top down” picture of the organisation.

- If there are two Auditors, the second Auditor can conduct One-to-One Interviews and/or Focus Groups while the first Auditor carries out the Functional Audit.

- During a One-to-One Interview, the Auditor is able to establish a relationship with the interviewee and elicit information about their job within the organisation. It is therefore very efficient to follow this immediately with a Process Audit of the interviewee’s work as this will capitalise on this relationship and eliminate the time required for basic introductions etc.

- If there is only one Auditor then they can conduct the One-to-One Interviews and/or Focus Groups followed by Process Audits once they have completed the initial Functional Audit.

3. Conduct of the Compliance Audit

The five key aspects of conducting a Compliance Audit are covered in the sections that follow and are also illustrated in flow chart form in Figure 3.5.

3.1 Opening Meeting

The purpose of the Opening Meeting is for the auditor(s) to meet the organisation's senior staff with responsibility for Data Protection and to make sure that they understand exactly what the auditor(s) intend to do. This can be achieved in a logical manner by using the Opening Meeting to confirm the following items:

- Scope of audit
- Audit Plan
- Meetings with staff, including closing meeting
- Personnel affected
- Reporting of findings
- Follow-up
- Practical arrangements

The suggested agenda for the Opening Meeting will be found in Annex D.2, and if it has been held correctly it will ensure that everyone involved in the audit will be in the right place, at the right time.

3.2 Audit Environment

Once the Opening Meeting has taken place, the main activity of the Compliance Audit can begin. However, it is very important at this stage to make sure that each component of the Compliance Audit takes place in the most suitable environment and with the most appropriate members of the organisation's staff.

3.2.1 Functional or Vertical Audit

This involves checking the operation of the Data Protection System within a particular area, function or department, and the Functional Audit Checklists of Annexes F, G and H will form the basis for this component of the Compliance Audit. It should be possible to work through a lot of these checklists in a conference room environment that could be where the Opening Meeting was held, the Audit Base Room itself, or somewhere similar.

It is also highly probable that the organisation's Data Protection Manager/Officer will be the best person to answer these questions, although other senior staff might need to be brought in to answer specific questions. There are, however, two important factors to consider at this stage:

- A conference room environment may be ideal for clarifying the details of the Data Protection System but will be inadequate for checking that it is actually being used in practice and that it is effective. These last two aspects of the Data Protection System can only be assessed adequately in situ by questioning the operational staff who actually perform the work.

- It is highly likely that any documentation that is brought into the conference room to answer a specific question will have been carefully selected beforehand as the best example. Auditors should always ask to be shown where the documents are kept and try and select their own samples.

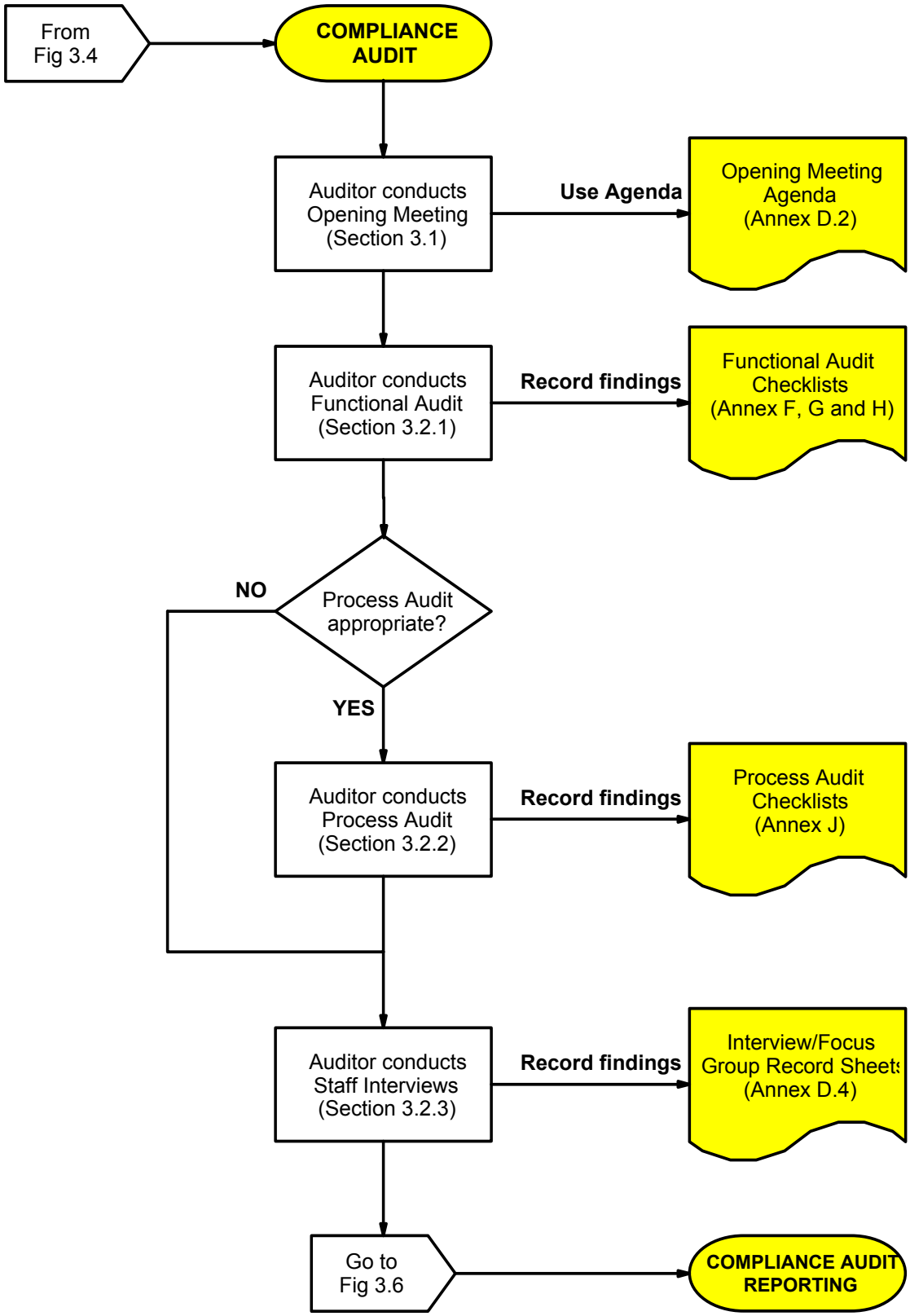


Fig. 3.5: Conduct of the Compliance Audit

3.2.2 Process or Horizontal Audit

This involves auditing a particular process that has Data Protection implications from beginning to end. This type of audit crosses interfaces between areas, functions or departments wherever they exist. It follows, therefore, that the Auditor will have to visit all the locations where the process in question can be seen taking place and this should have been clearly established at the Opening Meeting. It will also be very important for the Auditor to be able to directly question the members of staff who are actually carrying out the tasks. Any tendency for accompanying Heads of Department or Data Protection Managers to intervene and answer questions on their behalf should be strongly discouraged, unless specifically invited by the Auditor.

3.2.3 Staff Awareness Interviews

As well as checking the operation of the organisation's Data Protection Systems and related processes it is essential to assess the staff's awareness of Data Protection issues, particularly for those involved in the routine handling of personal data. This is best achieved via one-to-one interviews with the relevant members of staff, or via small Focus Groups.

These interviews are also a good opportunity to ask what Data Protection and related training has been received by the staff. The best environment for these sessions is a conference room, the Audit Base Room, or the office of the member of staff being interviewed if sufficiently private.

3.3 Audit Execution

The techniques used during the Compliance Audit will vary depending upon which particular component of the audit is actually being carried out. Recommendations for the most appropriate techniques to use for each component are discussed under the same headings as used for Section 3.2.

3.3.1 Functional or Vertical Audit

This type of audit concentrates on processes and procedures restricted to the department itself and does not cross inter-departmental boundaries. An example would be an audit of all the functions within a Personnel department. Section 3.2.1 has suggested that the Functional Audit Checklists of Annexes F, G and H should form the basis of this component of the Compliance Audit. Factors to consider when conducting a Functional Audit in this way include:

a) Questioning Techniques

For each question on the checklist always try and work through the following sequence:

- **Ask:** Ask the question to establish the facts
- **Verify:** Listen to the auditee's answer and verify where necessary that you have understood the actual situation
- **Check:** Confirm that what you have been told corresponds with what the Data Protection System actually says should occur. Also check that any associated records and logs are correct and up-to-date.
- **Record:** Write down your findings as described in the next section.

It is important that the Auditor is always prepared to change the order of questions from those drawn up in the checklists. This is to encourage the flow of information from the Auditee and so obtain the required information faster. This is why extra space is allowed on all the Checklists to record any supplementary questions and their corresponding answers.

b) Use of Checklists for Note Taking

Audit Checklists are the key records of what occurred during the audit and it is therefore essential that they should be used correctly. With reference to any of the checklists of Annexes F to J inclusive the columns should be used as follows:

- **Evidence (Documents) Examined:** The second column of the checklist is used to record details of the evidence presented in answer to the question. In the case of documents, reference numbers that uniquely identify them should be recorded such as procedure reference, order number, policy number etc.

- **Findings and Observations:** The third column is used by the Auditor to record their assessment of how well the evidence presented demonstrates compliance with the requirements of the Data Protection Act and the documented Data Protection System.

- **Result:** The final column of the checklist is used for grading the answer to each question, and the Auditor may choose to leave this activity until the end of the audit. Whenever the grading is done one of four categories are used (see 4.2 for details):

  - **COM:** The evidence demonstrates full compliance.

  - **MAJ:** The evidence demonstrates a Major Non-compliance.

  - **MIN:** The evidence demonstrates a Minor Non-compliance.

  - **OBS:** No Non-compliance was found but the Auditor has recorded an Observation about potential problems and how improvements could be made.

3.3.2 Process or Horizontal Audit

An example of this type of process would be a Data Subject Access request that covers more than one department, and the Process Audit Checklist of Annex J should form the basis of this component of the Compliance Audit. The conduct of a Process Audit is very similar to the Functional Audit and the following additional points should be taken into consideration:

a) Questioning Techniques

The same sequence of **Ask, Verify, Check, Record** should be used during the Process Audit. However, it is also very important to **Observe** what is actually happening once each question has been asked in order to **check** that this is in compliance with procedures.

b) Use of Checklists for Note Taking

The Process Audit Checklists will be used for note taking in a very similar manner to the Functional Audit Checklists, but the following additional points should be noted:

- **Evidence (Documents) Examined:** As well as recording reference numbers of any documents seen, this column of the checklist should be used for recording details of the process examined in terms of: **what, where, when** and **who.**

- **Findings and Observations:** This column should be used to record what the Auditor actually saw taking place, what the Auditee said, and the extent to which it complied with procedures.

c) Process Audit Strategy

Auditors will find it easier to conduct successful Process Audits if they adopt a consistent "walk through" strategy. By "walking through" the process in this way they will establish an Audit Trail that will show up any deviations from procedures. The recommended sequence of events is:

- The Auditor follows the procedure from one end to the other and can choose either:
  - **Trace Forward:** Start at the beginning and follow the entire process through to completion, e.g. start with a Subject Access Request and follow the process until the requested data has been despatched to the Subject.
  - **Trace Back:** Start at the end and follow the entire process back to the beginning, e.g. start with a completed Subject Access Request and trace it back to the original request from the Subject.
- If a discrepancy is found, the Auditor should report the symptom to the Data Protection Representative immediately for verification.
- If a discrepancy is found the Auditor should follow the trail through if possible until the probable causes are identified. This will make the Audit far more beneficial to the organisation rather than just reporting the symptoms. It should also provide helpful clues as to how the system might be improved to prevent errors recurring.
- The discrepancy together with any likely causes is then recorded on the Process Audit Checklist for later transfer to a Non-compliance Record as described in section 4.2.

3.3.3 Staff Awareness Interviews

During the Compliance Audit the Auditor needs to measure the awareness of Data Protection issues within the organisation, and the level of commitment to the Data Protection System. This is best achieved by assessing the attitude of management and employees to Data Protection either singly via one-to-one interviews or in small Focus Groups.

a) Interview Sample Size

When conducting one-to-one interviews or Focus Groups the Auditor(s) will have to decide how many staff should be included. The table below can be used to help determine a suitable sample size.

Total number of staff in area/ department being audited	Recommended sample size
1 – 5	100%
6 – 15	50%
16 – 50	25%
51 – 100	15%
101 – 500	10%
501 – 2500	5%

Auditors should realise that the above table is only a guideline and that the sample size should be altered depending upon individual circumstances.

b) One-to-one Interviews

The key features of the Interviews are:

- One-to-one format
- Duration of between 15 and 30 minutes

- Structured interview using directed questioning techniques
- Use of pre-set questions to establish:
  - Roles and responsibilities
  - Awareness of general Data Protection issues
  - Understanding of the Data Protection Principles directly relevant to their job
  - Understanding of the organisation's Data Protection System
  - Training received
- The interviewer's questions and the interviewee's answers are recorded on the Interview/Focus Group Record Sheet shown in Annex D.4

The recommended approach to conducting these interviews is for the Auditor to work through the questions on the Interview/Focus Group Record Sheet. These start off dealing with general aspects of Data Protection and then become more specific and ask about the interviewee's own work and training. The interviewee's answers and the Auditor's comments should be recorded on the sheet against each question.

c) Focus Groups

The key features of the Focus Groups are:

- Applicable in larger organisations or departments where many people carry out the same tasks
- Groups of between 3 and 6 staff
- Duration of about 30 minutes and one hour
- Group discussion facilitated by one of the Auditors using directed questioning techniques
- Use of pre-set questions to establish:
  - Roles and responsibilities
  - Awareness of general Data Protection issues
  - Understanding of the Data Protection Principles directly relevant to their jobs
  - Understanding of the organisation's Data Protection System
  - Training Received
- The interviewer's questions and the interviewee's answers are recorded on the Interview/Focus Group Record Sheet shown in Annex D.4

The recommended approach to conducting Focus Groups is very similar to one-to-one interviews except that the Auditor should adopt the role of a Facilitator rather than an Interviewer. This is to ensure that the members of the group do most of the talking while the Auditor keeps the conversation moving in the desired direction. The Auditor should also be aware that those who do not believe they know the answers to questions usually keep quiet, and this may give a false impression of the overall levels of knowledge of staff.

d) Outcomes

The results of both the One-to-one interviews and the Focus Groups are recorded in the same way as answers to checklist questions but using the Record Sheets shown in Annex D.4. The Auditor(s) need to analyse all of the completed Record Sheets and triangulate evidence between them in order to identify common trends and attitudes. For example, if the staff is fully aware of Data Protection Issues and how the system works it is likely to be efficient and well planned, and they will have received adequate training.

3.3.4 Positive Auditing

When recording observations on checklists during an Audit it is important to list everything that has been examined and not just those areas where problems or Non-compliances were noted. This is called “Positive Auditing” and is meant to give a balanced view of the whole Audit rather than just focussing on errors. For example, if five documents are examined and an error is noted on one of them, record the reference numbers of the four good documents as well as the one with the error. This practice will make the task of writing the Compliance Audit Reports much easier at the end of the Audit and will avoid giving an unfairly negative impression.

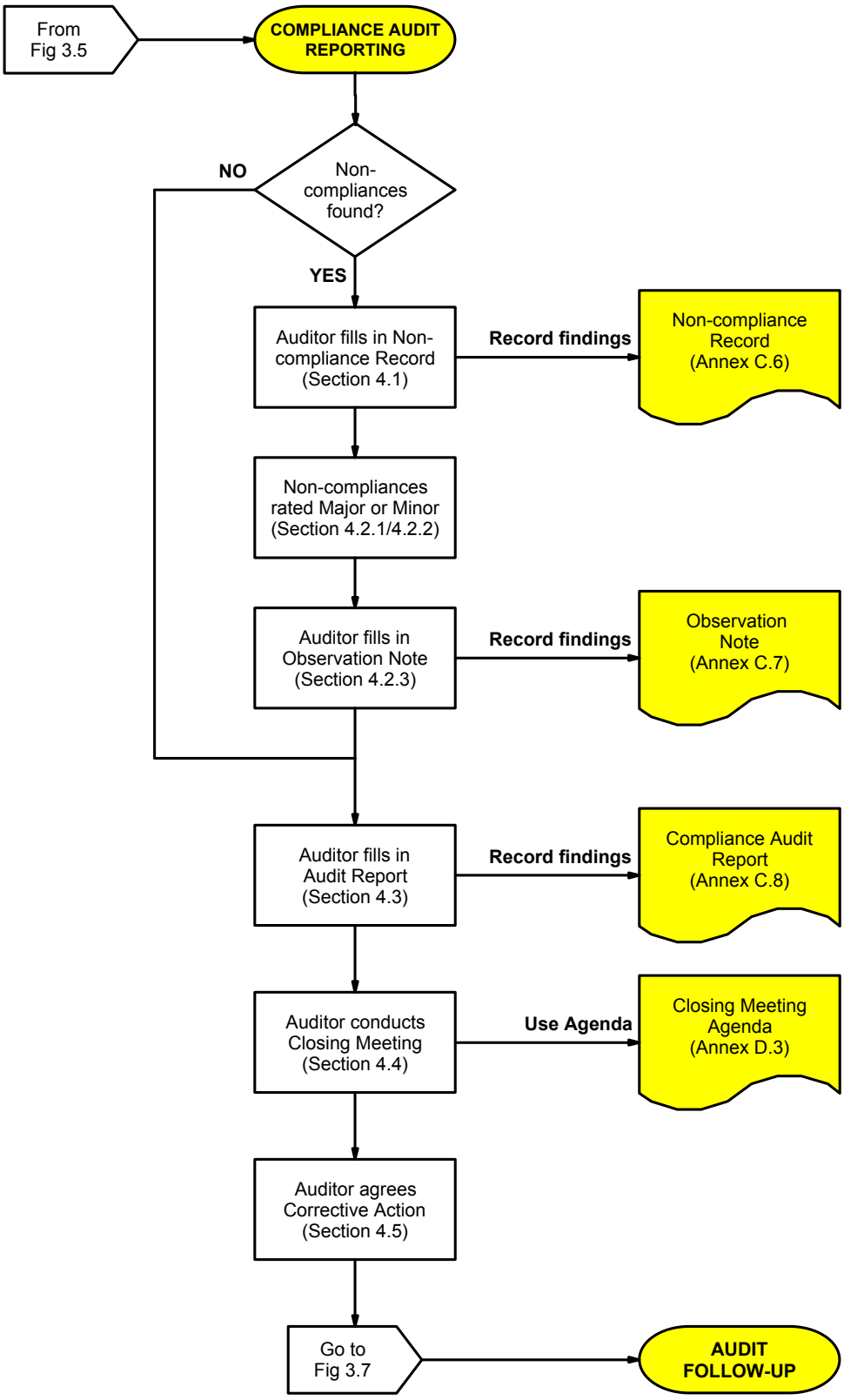


Fig. 3.6: Compliance Audit Reporting

4. Compliance Audit Reporting

The results of the Data Protection Audit must be documented in a formal manner and presented to the organisation at the end of the Audit. If the results of the Audit are documented correctly the organisation will be provided with much valuable information about the status of its Data Protection System and in particular:

- A formal record of what areas of the organisation were audited and when.
- An indication of those areas of the organisation that appear to comply with the requirements of the Data Protection Act.
- Details of those areas of the organisation that appear not to comply with the Act together with reasons for each non-compliance and their associated significance/risk.
- A suggested programme of corrective action including target dates to rectify any non-compliances found

The five key aspects of Compliance Audit Reporting are covered in the sections that follow and are also illustrated in flow chart form in Figure 3.6.

4.1 Non-compliance Records

Any Non-compliances discovered during the audit should be documented as soon as possible, ideally on the spot and certainly before the Closing Meeting. There should be sufficient detail in the report to clearly identify all the facts concerned especially the objective evidence. The information that needs to be recorded should, therefore, answer the following questions about each Non-compliance:

- What?
- Where?
- When?
- Why?
- Who?
- How?

It is recommended that a pro-forma is used for the Non-compliance Record and the suggested layout is given in Annex C.6 the key features of which are described in the following sections.

4.1.1 Header

The top section of the Record is used to document the following information about the audit:

- Audit reference
- Non-compliance reference
- Name of the organisation
- Name of the department (function or area as appropriate)
- Date of the audit

4.1.2 Details of Non-compliance

This section of the Record should carry sufficient detail about each non-compliance to answer the questions: What, Where, When, Why, Who, and How. It should also list the evidence found to substantiate the non-compliance in terms of records or documents seen, activities observed, or staff spoken to. This section is then signed and dated by the Auditor once the details of the non-compliance have been discussed and agreed at the Closing Meeting of Section 4.4.

It is important to realise that any occurrence observed that led to a non-compliance may have been the effect rather than the cause. The Auditor should therefore try to ensure that any evidence cited is objective and clearly relates to the causes of the non-compliance. An example of this would be where a data collection form does not provide an opportunity to decline unrelated uses of their information. The immediate "effect" of this is that clearly the form does not comply with the 1st Data Protection Principle. However, a good Auditor would delve deeper into the circumstances and investigate the organisation's form design and approval process. This might reveal that it does not include checking and sign-off by the Data Protection Manager, and that this is the ultimate "cause" of the non-compliance.

4.1.3 Corrective Action Programme

Each Non-compliance Record is discussed with the Data Protection Representative during the Closing Meeting in order to agree a Corrective Action Programme (see section 4.5). Once this has been done, the details of the Corrective Action Programme are entered onto this section of the form together with a proposed follow-up date. The name of the person responsible for the Corrective Action Programme should also be recorded in this section of the form that is then signed off by the Auditor and the Data Protection Representative.

4.1.4 Corrective Action Follow-up

The bottom section of the Non-compliance Record is used to record details of what the Auditor finds when the Audit Follow-up takes place and should include:

- Whether the agreed corrective action programme has been implemented
- Whether it has been effective in preventing recurrence of the non-compliance

Once the Auditor is satisfied with the corrective action they sign it off together with the Data Protection Representative as described in Section 5.4.1.

4.2 Non-compliance Categories

A Non-compliance will be recorded whenever the Auditor discovers that the organisation's Data Protection procedures are inadequate to prevent breaches of the Data Protection Act or they are adequate but are not being followed correctly. The Non-compliance Record pro-forma of Annex C.6 allows the Auditor to distinguish between two different levels of Non-compliance as follows:

4.2.1 Major Non-compliance

These occur in the following circumstances:

- Ongoing and systematic breaches of the Data Protection Act have been found.
- These breaches could have serious consequences for the individuals affected, e.g. a typographical error in personal data leading to a person being wrongly imprisoned overnight.

4.2.2 Minor Non-compliance

These occur in the following circumstances:

- One off breaches of the Data Protection Act have been found usually caused by human error.
- These breaches would have only a minor impact on the individuals affected, e.g. a typographical error in the spelling of someone's name causing annoyance.

It should be noted however, that a number of Minor Non-compliances in the same area can be symptomatic of a system breakdown and could therefore be compounded into a Major Non-compliance.

4.2.3 Observation

In order to make the auditing process as beneficial as possible to the organisation, it is always helpful for the Auditor(s) to record their observations about a particular process or activity. These observations might refer to potential problems that were noticed, or suggested improvements that could be made even though an actual Non-compliance was not found. For example, the organisation may not have a documented Subject Access Procedure and this could result in Subject Access Requests being delayed for more than 40 days if the person responsible for Data Protection happened to be on holiday.

It is recommended that a separate pro-forma, similar to a Non-compliance Record, is used for recording this information and the suggested layout of such an Observation Note is given in Annex C.7.

4.3 Compliance Audit Report

A Compliance Audit Report is produced after every Compliance Audit whether or not any Non-compliances have been discovered. The purposes of this Report are to:

- Record the key reference data relating to the Data Protection Audit such as date, scope, areas assessed, name of audit team etc.
- Summarise the main findings of the audit and refer to any non-compliances identified
- Document suggestions for any corrective action whether agreed or not
- Record the nature and timescale of any agreed follow-up visits.

A pro-forma may be used for this report and a suggested two-page layout is given in Annex C.8, the key features of which are described in the following sections. There are many benefits to finalising and delivering the compliance audit report in the field at the end of the audit. However this will depend upon the nature of the information received during the audit and the complexity of the compliance issued raised.

4.3.1 Header

The top section of the first page of the Report is used to record the following information about the audit:

- Audit reference
- Name of the organisation
- Name of the department (function or area as appropriate)
- Date of the audit

4.3.2 Audit Summary

The main section of the first page is used to summarise the results of the audit. The summary should be factual and fair and must reflect that it is ultimately only a "snapshot" of the situation taken at a particular time and place. However, it may be helpful to the organisation to state in what way the situation has changed since the last audit, i.e. is it improving, getting worse or static.

It is also very important to ensure that the summary is as ***evaluative*** as possible and not merely ***descriptive***. After all, the organisation does not need to read a lengthy description of its Data Protection Policies and Procedures – it knows this information already. What it doesn't know is how good and effective they are, and this is what the summary needs to evaluate.

Auditors will find it quicker and easier to write these summaries in the form of a template consisting of a number of standard paragraphs. It is suggested that each paragraph could be structured to record the following information:

a) First Paragraph

This paragraph should cover the scope of the audit and include:

- The names of areas, functions or departments visited, and the processes audited.
- If an adequacy audit has been undertaken the results of this should also be stated
- Total number of Major and Minor Non-compliances raised and number of Observations recorded.

b) Second Paragraph

This paragraph should document the results of the Functional Audit, and include:

- Brief description and evaluation of the Data Protection System in terms of organisation, management and documentation at the corporate level.
- Brief description and evaluation of how the Data Protection System operates at departmental level and how it interfaces with the corporate system.
- Comment on how the Data Protection Principles have been dealt with and evaluate any special features or problems.

c) Third Paragraph

This paragraph should document any special aspects of the Functional Audit, and include where applicable:

- Evaluation of the use of Data Processors.
- Evaluation of the Notification systems.
- Evaluation of Transitional Arrangements.

d) Fourth Paragraph

This paragraph should document the results of any Process Audits, and include:

- Brief description and evaluation of each process audited.
- Number of items, documents, records etc. inspected.

e) Fifth Paragraph

This paragraph should document the results of the One-to-One Interviews and/or Focus Groups and include:

- Total number of One-to-One Interviews and/or Focus Groups held.
- Evaluation of staff commitment to personal privacy and awareness of data protection issues.
- Evaluation of quantity and effectiveness of staff data protection training.

f) Final Paragraph

The last paragraph should give the Auditor's overall evaluation of the effectiveness of the organisation's Data Protection System. Comment can also be made about the organisation's general ethos concerning information confidentiality and data security. Finally, the Auditor could note how the situation has changed since the last audit.

4.3.3 Summary of Corrective Actions

The top half of the second page of the Audit Report is used to summarise all the Non-compliances raised during the audit and records the following information for each:

- The Non-compliance reference number
- Who is responsible for carrying out the corrective action
- The agreed corrective action to be taken
- The date when the corrective action will be completed

4.3.4 Agreed Audit Follow-up

The bottom half of the second page of the Audit Report records the agreed follow-up action in terms of its scope and timescales as described in Section 4.4.4.

4.4 Closing Meeting

The purpose of this final meeting is for the Auditor(s) to present their findings to the organisation's key data protection staff. The meeting should be quite brief and it is recommended that the Auditor chairing the meeting should cover the following points:

- Thank the organisation for their assistance, co-operation and hospitality
- Presentation of Audit summary and detailed findings
- Post Audit reporting
- Arranging the nature and timescale for any required Audit follow-up

It is also worth emphasising at the beginning of the meeting that an Audit can only be a snapshot of activities and is therefore subject to the risks associated with sampling. Only a selection of activities was assessed and so there is always a possibility that non-compliances exist in areas not covered by the Audit.

The suggested agenda for the Closing Meeting will be found in Annex D.3 and the key actions for the Auditor chairing the meeting are described below.

4.4.1 Confirmation of Non-compliances

Section 4.2.2 has explained how the details of each Non-compliance found are recorded on a separate Non-compliance Record form. It is recommended that the Auditor read out each one individually during the meeting so that they can be confirmed by the Data Protection Representative and signed off by the Auditor.

4.4.2 Agreement to suitable Corrective Action

It is the responsibility of the organisation's management to propose a suitable corrective action programme for each Non-compliance discovered during a Data Protection Audit. Although it is not the Auditor's role to offer advice or guidance to the organisation during an audit, it is essential that they are satisfied that the proposed corrective action will actually remove the Non-compliance. Advice or guidance could be offered during the post-audit reporting phase.

If we return to the example given in Section 4.1.2 it can be seen that had the bad design of the form been cited as the non-compliance, a logical programme of corrective action would be to re-design the form. Although this might correct that particular form it would not necessarily prevent other forms from exhibiting similar problems. However, if the form design and approval process had been cited as the non-compliance, the logical corrective action would be to include the Data Protection Representative in the sign-off loop. It can be seen that this would not only correct the form in question but would also ensure that all forms were designed correctly in future.

Once the proposed corrective action has been agreed it is documented in the middle section of the Non-compliance Record itself as described in Section 4.2.3, and then signed off by the Auditor and the Data Protection Representative.

4.4.3 Corrective Action Responsibilities and Timescales

The middle section of the Non-compliance Record should also be used to record the name of the person responsible for carrying out the Corrective Action programme. During the Closing Meeting the “Follow-up Date” box of the Non-compliance Record should be filled in specifying the date by when the Corrective Action will be completed and ready for review.

4.4.4 Agreed Audit Follow-up

Once the top two sections of each Non-compliance Record have been completed and signed off, the Auditor should agree what form any Audit Follow-up should take and when it should take place. Guidelines for deciding this are given in Sections 5.1 and 5.2. This information should then be recorded in the lower section of the Compliance Audit Report, which can then be signed off, by the Auditor and the Data Protection Representative.

4.5 Audit Report Distribution

Once the Compliance Audit Report and any associated Non-compliance Records and/or Observation Notes have been signed off, they should be provided to the Data Protection Representative so that they can proceed with the Corrective Action programme. The individual Non-compliance Records can then be completed and signed off as described in Section 5.4.1, and finally the Compliance Audit Report can be signed off and the Audit closed as described in Section 5.4.2.

Once the Audit is closed the Data Protection Representative should hold the originals of all the documents in an Audit File. The person responsible for the function or area covered in the Audit Report might also wish to retain copies for reference purposes.

4.6 Audit with no Non-compliances

If no Non-compliances are found during an Audit then the “Summary of Agreed Corrective Actions” and the “Agreed Audit Follow-up” sections of the Compliance Audit Report should be left blank (see sections 4.1.3 and 4.1.4). The Audit can then be completed by the Auditor and the Data Protection Representative signing off the “Audit Closed” section at the foot of the Compliance Audit report during the Closing Meeting.

5. Audit Follow-up

If any Non-compliances are discovered during a Data Protection Audit, it is desirable to undertake some sort of Audit Follow-up in order to check that the proposed corrective action has actually been implemented and that it has been effective.

The issues that need to be addressed when deciding on an appropriate Audit Follow-up programme are described in the sections that follow and are also illustrated in flow chart form in Figure 3.7.

5.1 Scope

The scope of follow-up action should be chosen in accordance with the severity of the original non-compliance and therefore may be any of the following:

- Confirmation via telephone of minor adjustments.
- Documentation checks.
- Partial re-audits only covering those areas where Non-compliances were recorded.
- Full re-audit of entire Area/Department where a substantial lack of adequate controls or systematic disregard of procedures was found.

This information will be recorded in the lower section of the Compliance Audit Report during the Closing Meeting as described in Section 4.4.4.

5.2 Timescales

The timescale of the follow-up action should also be chosen in accordance with the severity of the original Non-compliance and the original risk assessment of the Data Protection activities involved (see Section 1.1). Minor non-compliances may be left until the next scheduled audit of the Area/Department while major problems may need to be corrected immediately. This information will also be recorded in the lower section of the Compliance Audit Report as described in Section 4.4.4.

5.3 Methodology

The choice of methodology for the Follow-up Audit will very much depend upon the scope as described in Section 5.1. If the Follow-up involves checking only documentation then an Adequacy Audit of Section 2.1 would be sufficient. If a site visit is involved because of the seriousness of the Non-compliances, then the Auditor(s) may choose any or all of the Compliance Audit techniques dealt with in Section 3.3, i.e.:

- System or Vertical Audit
- Process or Horizontal Audit
- Staff Awareness Interviews.

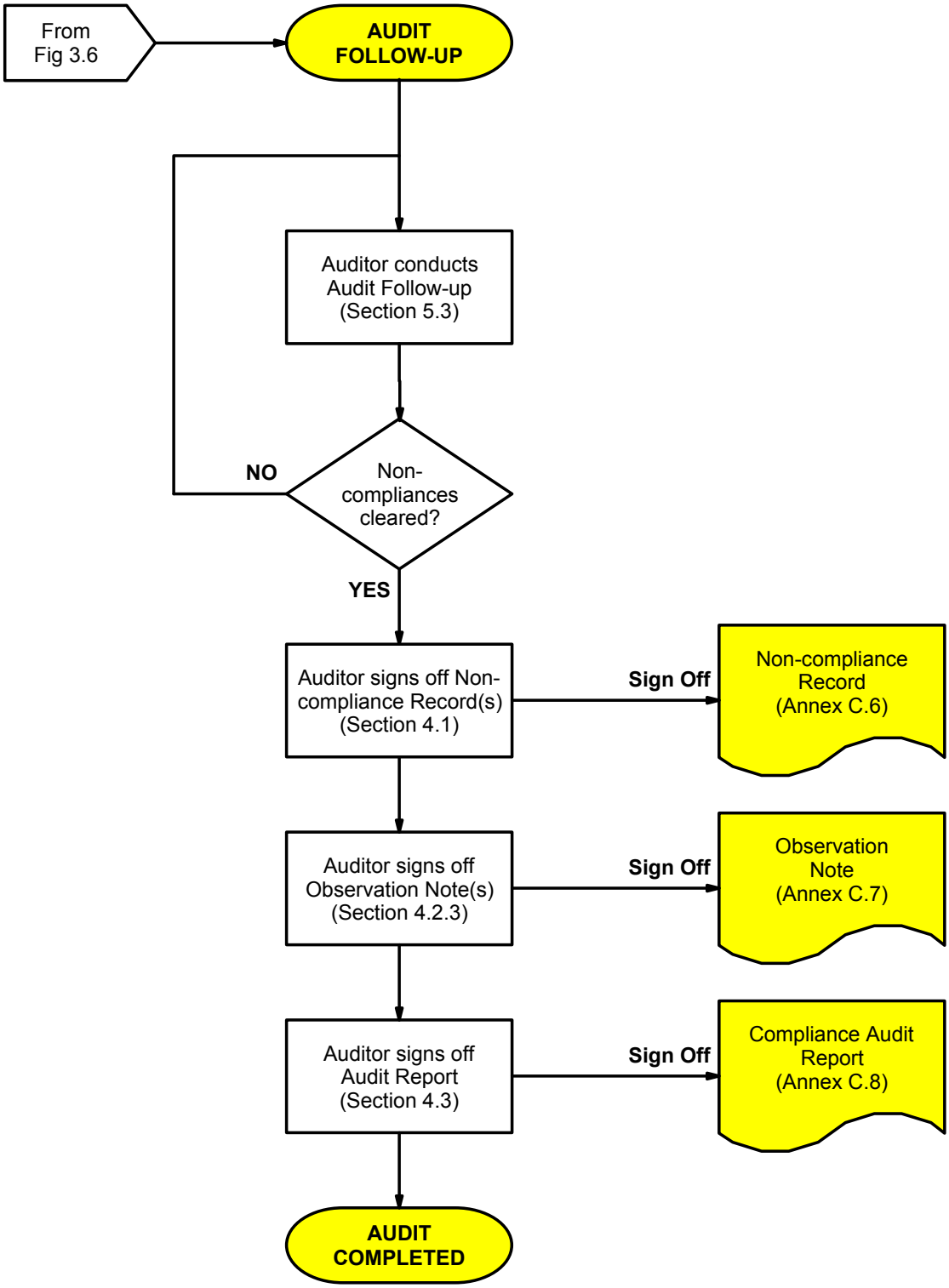


Fig. 3.7: Audit Follow-up

5.4 Audit Closure

Once all the necessary Corrective Action has been checked by the Auditor and found to be satisfactory, the Audit can be formally "closed" and this will involve the following activities.

5.4.1 Non-compliance Sign-off

During the Follow-up Audit, the Auditor checks the Corrective Action that has been implemented for each Non-compliance found during the original Audit. The details of how the Corrective Action has been implemented and whether it has been effective are then recorded at the bottom of the Non-compliance Record. Once the Auditor is satisfied with these findings the Non-compliance Record is signed off by the Auditor and the Data Protection Representative.

5.4.2 Compliance Audit Report Closure

Once all of the Non-compliance Records associated with an Audit have been signed off as described in Section 5.4.1, the bottom section of the Compliance Audit Report can be signed off by the Auditor and the Data Protection Representative. This will then formally close the Audit.

Part 4: Guide to Auditing

Part 4: Guide to Auditing

Illustrations

Part 4: Guide to Auditing

Section 1.3.3 of Part 3 of the Audit Manual mentions that Internal Auditors, particularly those in smaller organisations may not have received formal training in Auditing. However, the Information Commissioner wants to encourage all organisations to include Data Protection compliance within Internal Audit Programmes to help them monitor and improve their level of compliance with the Data Protection Act. Therefore, the purpose of this Part of the Audit Manual is to provide enough practical advice and guidance so that even novice auditors will have sufficient confidence to go out and conduct a Data Protection Audit without necessarily having attended a formal training course

1. The Role of an Auditor

Before defining the skills required by Auditors it is worth recalling what the role of the Auditor is when conducting a Data Protection Audit. The key roles identified from the earlier Parts of this Manual include:

- Checking the current compliance status
- Assessing the staff's awareness of their data protection obligations
- Assessing whether the rights of Data Subjects are adequately protected
- Identifying non-compliances
- Agreeing suitable corrective action to remove non-compliances.

It is also worth bearing in mind the following aspects of the audit process while reflecting upon the role an Auditor is required to undertake.

- Any person who conducts an audit must do so with the full authority of the executive management. Otherwise, they may find that their authority is challenged by people who are senior to them.
- The internal audit process requires commitment.
- Ideally, Auditors should be supported by more experienced colleagues when first conducting audits.
- Auditors should be independent of the function being audited, and should be objective when undertaking audits.

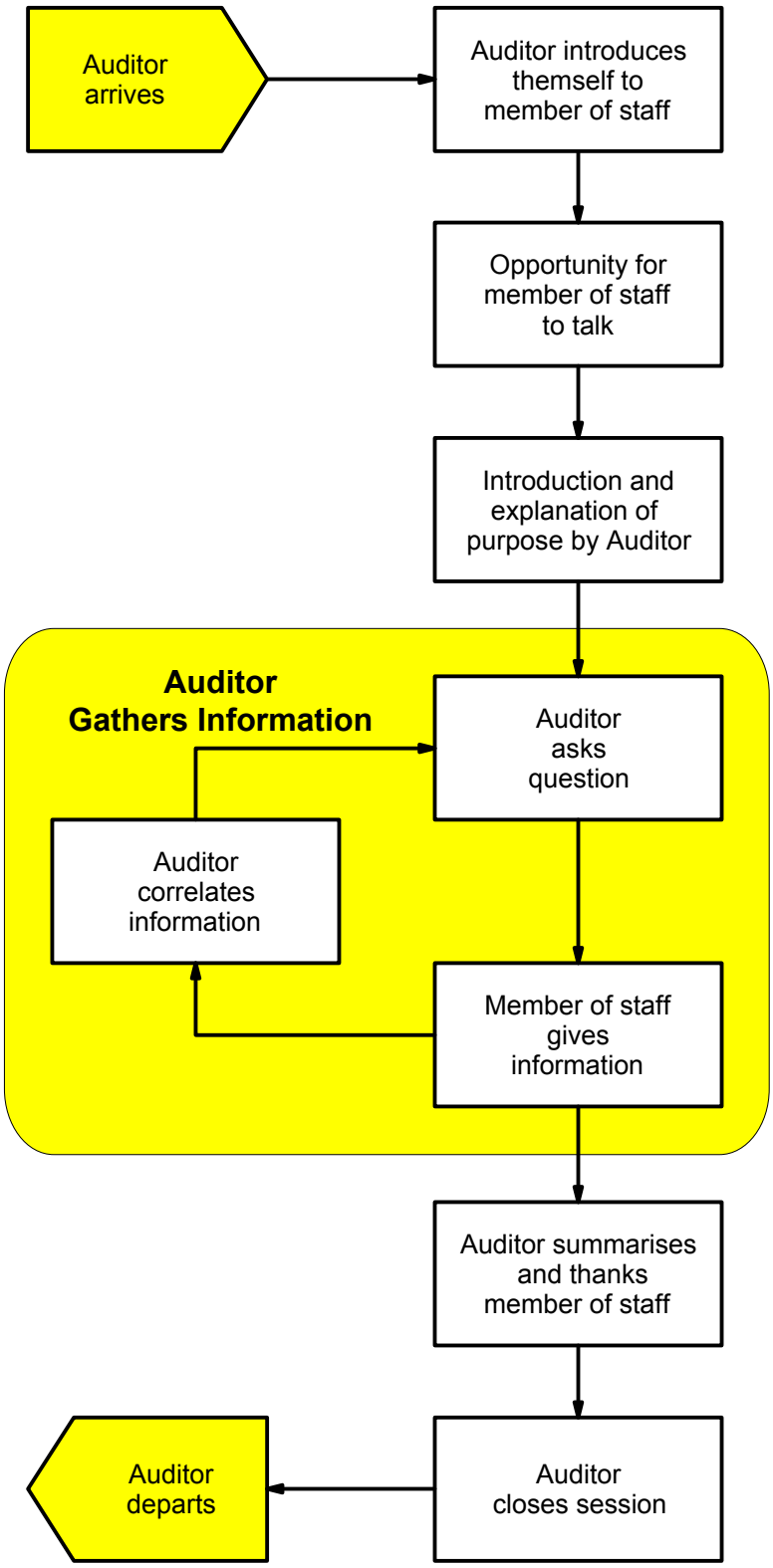
2. Auditing Tasks

It is also worth recapping on the tasks faced by a Data Protection Auditor before looking in detail at the skills required and the techniques that can be applied. The key tasks are:

- Obtaining and assessing objective evidence fairly
- Arriving at generally acceptable conclusions based on audit observations.
- Remaining true to a conclusion despite pressure to change that is not based on objective evidence
- Conducting the audit process without deviating due to distractions
- Committing full attention and support to the audit process
- Constantly evaluating the effects of audit observations and personal interactions
- Reacting effectively in stressful situations
- Treating the staff involved in a way that will best achieve the audit objectives

The first four items in this list broadly relate to the mechanics of auditing while the last four are more to do with the human aspects of auditing. These human aspects will be dealt with in more detail in section 3 so that this section can concentrate more on the actual process of auditing.

Fig. 4.1: Interview Structure



2.1 Obtaining Evidence

Auditors should never lose sight of the fact that the fundamental purpose of any type of audit is to obtain objective evidence. A certain amount of evidence will be obtained by reviewing documentation as in the initial Adequacy Audit. However, evidence of whether the Data Protection System is actually understood and being used by staff can only be established by asking direct questions. In a way, talking to a member of an organisation's staff to obtain information is similar to conducting an interview. Obviously, the Auditor will want to keep the process as relaxed an informal as possible, but it is probably helpful to approach each information gathering session as if it were a simple, structured interview.

The sort of interview structure recommended for use during audits is shown graphically in Figure 4.1, and the key components of this are described below.

2.1.1 Auditor Introduction

The Auditor should always start off the session with a warm greeting to the member of staff and thank them for giving up their time to participate in the Audit.

2.1.2 Opportunity for Member of Staff to Talk

The Auditor should then try and relax the member of staff by giving them an opportunity to talk. This is best achieved by asking some innocent but relevant questions such as how long they have been doing their particular job etc.

It should be remembered that most people find the process of being audited stressful even if it is being done by someone within the organisation that they already know. It is considerably more stressful for the member of staff when the Auditor is from an outside organisation as is the case for a second or third party audit.

2.1.3 Explanation of Purpose

It is always a good idea at this point for the Auditor to explain the purpose of the Audit and the structure of the information gathering session. This should set the member of staff's expectations in terms of the areas to be covered and the time available. It is always courteous to check that the proposed structure is acceptable to the member of staff.

2.1.4 Auditor Gathers Information

This section should form the main body of the session and as a rule of thumb should take up about 90% of the total time available. During this part of the session the member of staff should be talking for approximately 80% of the time and the Auditor for no more than 20%.

2.1.5 Information Correlation

As well as listening to the member of staff's replies the Auditor should be aware of non-verbal signals to see how well they correlate with what is being said, e.g.:

- Eye contact,
- Body posture (e.g. nodding, leaning forward etc.)
- Behaviour.

In particular, signs of irritation or stress should be looked for as these could indicate that the member of staff is unhappy about the area being discussed and their consequent answering.

2.1.6 Summary and Closing

The Auditor should conclude the session in a courteous manner by:

- Summarising the key points that have emerged during the session
- Thanking the member of staff for an interesting discussion
- Thanking them (again) for giving up their time to attend the session

It should be noted that this structure could also be used for conducting both one-to-one interviews and focus groups with staff to assess their levels of data protection awareness.

2.2 Assessing the Evidence

Once the evidence has been gathered it has to be assessed objectively by the Auditor to decide whether it demonstrates compliance with the requirements of the Data Protection Act or not. While carrying out this assessment the Auditor should bear the following points in mind.

2.2.1 Sources and Reliability

It is very important that the evidence gathered is of high quality if it is going to be used to make a robust judgement. The source of the evidence will be a significant factor affecting its reliability, and it may come from a variety of places including:

- Documentation
- One-to-one interviews
- Focus Groups

When assessing the reliability of documentary evidence an Auditor should take various factors into account such as whether it is a formal or informal document, its age, authorship and distribution within the organisation.

When assessing the reliability of information obtained from staff in interviews or focus groups it should be remembered that in these situations people can be argumentative, undisciplined, dishonest, opinionated, impatient, inarticulate, lazy, apathetic, domineering or downright rude. Equally, auditees might appear to be very helpful and co-operative because they are trying to tell the Auditor what they think they want to hear.

2.2.2 Weaknesses in Information

The previous section has dealt with some of the factors that may affect the reliability of any information gathered during an audit from the point of view of its origin. It is also important to take into account any lack of objectivity that might be introduced by the Auditor themselves. For example:

- Are they bringing any “baggage” with them from their own organisation or other organisations that they have audited in the past?
- Are they trying to impose their own ideas of best practice?
- Are they looking for an unachievable “gold standard” rather than assessing compliance with the Act?
- Have they allowed an initial impression gained from the Adequacy Audit to narrow the subsequent evidence gathering during the Compliance Audit?

All of these factors may cause an Auditor to lose their objectivity and need to be guarded against carefully when assessing evidence.

2.2.3 Strengthening the Evidence Base

If an Auditor is to make a robust judgement then there needs to be a strong evidence base on which to make that judgement. The factors that will help to strengthen evidence include:

- **Multiple Instances:** The Auditor should check whether what they have found is an isolated, "one off " incident or whether it is systematic. One off incidents can often be put down to human error, whereas multiple or systematic occurrences frequently indicate a breakdown of a particular system or process.
- **Triangulation:** The Auditor should also seek to triangulate evidence from different sources to strengthen their findings. For example, is there independent corroboration about a particular piece of evidence from different members of staff obtained during different interviews or focus groups? Can the existence of a particular activity be confirmed from two or more separate documents?

2.2.4 Validity, Reliability and Repeatability

A useful final check for a piece of major evidence that is going to be used as the basis for a non-compliance is to subject it to a Validity, Reliability and Repeatability test as follows:

- **Validity:** Make sure that the evidence presented is really valid for the area being assessed. For example, does it come within the scope of the Data Protection Act?
- **Reliability:** Ensure that the evidence is accurate and consistent and not subject to any of the flaws mentioned in sections 2.2.1 and 2.2.2.
- **Repeatability:** Ask yourself whether another Auditor would arrive at the same conclusion when presented with the evidence that has been found.

3. Human Aspects

Having looked a little at the mechanics of auditing in section 2, we now turn to the more human aspects of auditing. Recalling that a lot of compliance auditing involves gathering information by talking to members of staff we will discuss which behavioural characteristics are desirable in an auditor and provide advice and guidance on best practice.

Organisations should be aware that it could take days of intensive training to provide a prospective Auditor with basic questioning, active listening and body language interpretation skills. A comprehensive treatment of these subjects is obviously beyond the scope of this Manual and organisations who need further guidance on this type of training should contact an appropriate training company for more information. The following sections, however, highlight the key aspects of human behaviour that should be considered when carrying out Audits.

3.1 A Good Auditor

It is possible to identify some basic behavioural characteristics that all Auditors should aspire to. Hopefully most of these will be self-explanatory, but it is always useful to keep the attributes in the list below at the back of your mind when on an audit:

- **Objective:** An Auditor must only deal with facts. You will be lost if you ever lose your objectivity during an audit.
- **Fair:** An Auditor must always be fair and report exactly what they have discovered during an audit without fear or favour. You have obligations to the Data Protection Representative, the organisation and auditees when conducting an audit. If it is an internal audit then these people are likely to be colleagues so it is important to be professional.
- **Thorough:** The organisation and its staff will probably have put a lot of time and effort into preparation before the audit. It is therefore important that they feel that the Auditor has made a thorough job of examining everything covered by the assessment. Equally, the more preparation the Auditor has done beforehand the more thorough the Audit will be as a result.

- **A good communicator at all levels:** On a typical audit an Auditor may be dealing with senior management, heads of department and office staff. It is therefore important that you are able to communicate effectively at all strata within an organisation and don't "talk down" to junior staff or be obsequious with senior staff.
- **Friendly:** Auditees will always react better to a friendly Auditor. When trying to decide just how friendly you should be remember that you are in effect a visitor or guest. Therefore you should try and only do or say things that would be acceptable for a guest otherwise your behaviour may cause concern and provoke an adverse reaction among the staff.
- **Patient:** Remember that the process of being audited puts the organisation and its staff under a lot of stress. You must therefore make allowances for this when people don't react quite as quickly as you think they should.
- **Determined:** You have to be fairly single minded to achieve the objectives of an audit and settle any doubts without distraction. However, this does need to be balanced by a degree of pragmatism. For example an Auditor who is determined to find fault at any cost may spend hours on endless "nit picking" which is a waste of everybody's time and money.
- **Calm under pressure:** Auditing involves quite intense work being carried out over sustained periods. You have a lot to get through with rigid deadlines, and during the audit will probably not be able to stop at 5 pm each day. You must therefore be able to work calmly under pressure to reassure the auditees that everything is "under control" at all times.
- **Calm when provoked:** We have said in section 2.1.2 that auditees may be argumentative, undisciplined, opinionated, impatient, domineering or downright rude. It is essential that if you as Auditor are faced with a member of staff who behaves like this that you do not react if provoked but stay calm, polite and in control.

3.2 Good Practices

Section 3.1 has listed some of the attributes that good Auditors should have to help them do the job. There are also a number of practical steps that the Auditor can follow to make the process as positive, helpful and efficient as possible. Examples of good practices for Auditors include:

- **Ask the right person:** Always check that you are talking to the person who can best answer your questions. Don't waste time with people who are not involved with the task or are not responsible for it.
- **Look at the person:** When you are speaking to the right person, always look at them when asking your questions. They will find it easier to understand and you will be able to judge better whether they have understood by studying their facial expression.
- **Speak clearly and simply:** Auditees will have difficulty following long and complex questions so try and speak clearly and keep the questions as simple as possible.
- **Rephrase the question if necessary:** If you can see that the auditee has not understood your question, try and rephrase it and ask it again.
- **Smile and be relaxed:** You want to appear friendly to the auditee so smile when introduced. They will also feel more relaxed if you are.
- **Be unemotional and impartial:** Remember that your role is to make judgements based on objective evidence.
- **Do not look for trouble:** People may become quite aggressive if you find a Non-compliance. Once you have established the basic facts and the likely root cause move on so that staff do not feel they are being victimised.
- **Do not project superiority:** You must resist the temptation to be overbearing and throw your weight around due to the authority that has been invested in you as an Auditor.
- **Give praise when deserved:** Although your task as Auditor is to judge how effective the data protection system is at preventing errors you must guard against it appearing a search for failure. Try to be as positive as possible and where you see examples of good practice always give credit where credit is due.

3.3 Bad Practices

As well as adopting the good practices listed in section 3.2, Auditors should try and avoid the following bad practices:

- **Ask too many questions at once:** Ask one question at a time and only move on once you have received the answer or else you will confuse the auditee.
- **Say they understand when they don't:** Don't be afraid to ask the auditee to explain something they have said if you do not understand. You are not expected to be an expert in everything.
- **Answer their own questions:** Let the auditee answer the question; don't put words into their mouth.
- **Give insufficient time to answer:** Although you will be under a lot of time pressure you must give the auditee sufficient time to answer each question.
- **Get into an argument:** This is a consequence of looking for trouble discussed in section 3.2 and should be avoided at all costs.
- **Rely on their memory:** All your questions should be written down on your checklists, so make sure that all the answers are too. Then you won't have to rely on your memory when it comes to writing up Non-compliance and Audit reports afterwards.
- **Give subjective opinions:** Remember first of all you have to be objective, and secondly you are not really there to give advice but to make judgements based on the evidence.
- **Take sides:** You have to be impartial at all times.
- **Criticise individuals:** Your role as Auditor is to assess the effectiveness of the data protection system not individuals. If you do find evidence of a breach of the Data Protection Act first establish whether it is due to a system failure. If it is due to human error check whether the individual has had sufficient training to carry out the task. If they have not been trained sufficiently then this is also a system failure.

You will find that the best way of avoiding many of the above bad practices is to be very careful about the way you respond to answers provided by auditees. This is illustrated by the phrases shown below which are likely to lead to the undesirable consequences indicated and should be avoided by the Auditor.

Phrase	Likely consequence
If I were you	Subjective opinion
When I was at	Auditor's "baggage"
If you do this	Giving advice
Fine, but	Getting into an argument
I told you so	Criticising

3.4 Establishing Relationships

We have already said that a large part of auditing involves gathering information by asking people questions. This process will be made much easier and quicker if the Auditor can quickly establish a relationship with the auditee right from the beginning. The following techniques should help Auditors with establishing relationships:

- **Developing an interest with sincerity and friendliness:** People always respond better if they feel that you are interested in what they are doing or saying.
- **Making the auditee the central figure:** Ensure that the auditee has ample opportunity to provide you with the information sought.
- **Recognising their own prejudices:** What you see may not correspond with the way you would like to see things done. However, your job is to check that it is being done the way the organisation wants it, and it complies with the requirements of the Data Protection Act.
- **Being careful in giving advice:** The main reason you are there is to function as an Auditor, not a consultant.
- **Recognising that people only hear what they want to hear:** We are all guilty of this so make double sure that your comments are understood. Ideally, the major points you are trying to get across will be written down either on a Non-compliance Report or the final Audit Report so there is no uncertainty or ambiguity.
- **Listening to understand:** Don't just hear the words being said but make sure you understand the meaning behind them.
- **Being sensitive to feelings, attitudes and motives:** Inter-personal sensitivity is a key skill in activities like Auditing as it involves so much one-to-one interaction with people.
- **Responding in a neutral manner:** Remember to be impartial.
- **Repeating or rephrasing something they have said:** The best way of checking that you have understood something is to try and say it back to the auditee in your own words.
- **Using questions carefully:** You will have spent a long time preparing your checklist questions if you are conducting a Process Audit, so make sure they are used effectively.

4. Audit Techniques

Staff who are new to auditing will need some simple and practical guidance on the basic techniques used when conducting an audit. Section 3.3.1 of Part 3 has introduced the topic of how to ask questions during an audit to make the process as effective as possible. This section will provide Auditors with more help with basic questioning techniques.

4.1 Basis of Questions

Auditors should remember that all the questions used during an Audit should be based either on the organisation's own data protection system documentation, or the requirements of the Data Protection Act. Therefore:

- Do not refer to "good practice"
- Do not express personal preferences

You are there to check whether the practices and activities throughout the various areas of the organisation comply with the documented data protection system, and whether this adequately meets the requirements of the Data Protection Act.

4.2 Good Questioning Techniques

The process of gathering information during an Audit will be made more effective by giving careful thought and attention to the way that you actually ask questions. Auditors should find it helpful to be aware of the following techniques:

4.2.1 Open Questions

An "open" question is one that cannot be answered with a simple "yes" or "no" and prompts the member of staff to provide further information. "Open" questions usually begin with any of the following:

- What? Why? Where? When? Who? How?

Other good ways of starting open questions include:

- Can you show me?
- What if? (but try not to be too hypothetical)

4.2.2 Directed Questioning

Directed questioning is a technique where the Auditor starts off with a general opening question on a particular topic and follows this up with a sequence of further questions each of which is narrower in scope than the previous one. The final question in the sequence should then end with the member of staff giving a specific answer to the question posed.

4.2.3 Inviting a Negative Response

Staff often feel under a lot of pressure to always answer questions positively during an audit. The Auditor should try and make it acceptable to admit to something negative by careful posing of the question. For example, staff would invariably answer the following question in a positive way (i.e. with a "no"):

- Have you ever made a mistake in your job?

This question could be rephrased as follows to make it acceptable for the member of staff to admit to making errors with a "yes" answer:

- It is only human to make the occasional slip-up in our jobs, can you describe to me an occasion when you made a slight mistake recently?

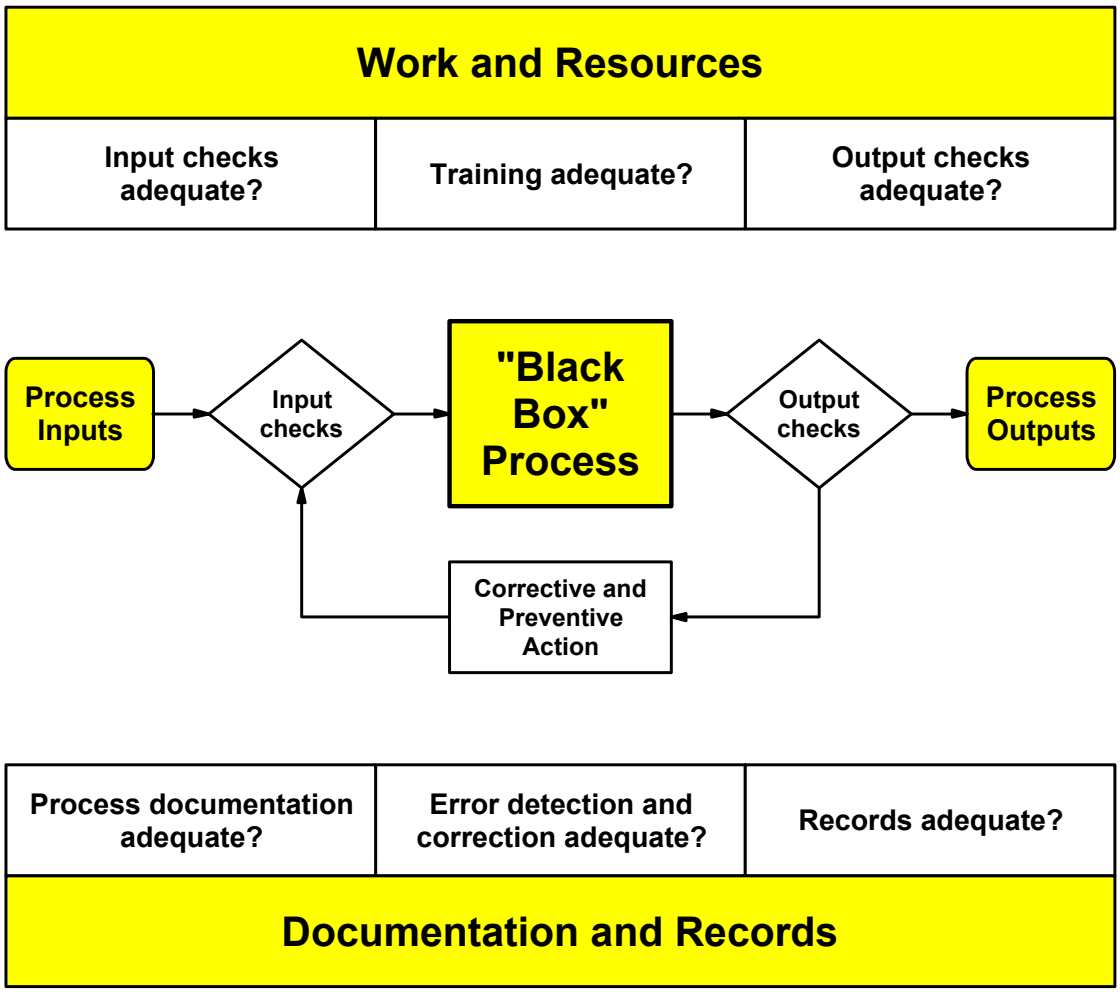


Fig. 4.2: Black Box Audit Model

4.3 Questions to Avoid

The quality of information gathered from an audit will be higher and the amount of time taken to get it will be reduced if some bad practices are avoided.

4.3.1 Closed Questions

A "closed" question is one that the member of staff can answer with a simple "yes" or "no". This will provide very little information to the Auditor and will not provide a natural lead on to the next question. "Closed" questions can have a role to play, though, in controlling the timing of an interview if required.

4.3.2 Limiting Questions

A "limiting" question is one where the Auditor has presented the member of staff with two or more possible answers to a question. The limiting of the member of staff's scope in answering in this way is little better than using a "closed" question as in section 4.3.1 above.

4.3.3 Hypothetical Questions

There is very little value to be obtained in asking a member of staff a hypothetical question or inviting them to speculate about their reactions in a situation of which they have had no experience.

4.3.4 Leading Questions

A leading question is one that attempts to force the member of staff to provide the response that the Auditor wants to hear rather than what they actually want to say. Again, this type of question is of very little value in an audit situation.

4.3.5 Multiple Questions

Inexperienced Auditors often ask a question and before the member of staff has had a chance to reply they follow it up with one or two further questions. This is very confusing to the member of staff as they are presented with a choice of questions to answer and may not answer the most important one.

4.4 Black Box Auditing

It is quite possible that an Auditor may be asked to audit a complex and technical process with which they have little familiarity. In these circumstances it may be helpful for the Auditor to think of the process to be audited as a “Black Box” where the staff carrying out the process have been trained to operate within the “Box”. The Auditor does not have to be an expert at the detailed technical operations within the “Box” but needs to check that the overall process complies with the requirements of the Data Protection Act in terms of:

- Are the inputs to the process adequately checked?
- Are the outputs from the process adequately checked?
- Is the process itself adequately documented consistent with the expected skill levels of the staff involved?
- What happens when errors occur?
- Are the records adequate to show that work has been processed correctly?
- Have the staff been adequately trained to carry out the process?

This “Black Box” audit model is illustrated graphically in Figure 4.2

5. Practical Considerations

The novice auditor will feel more confident and relaxed if they arrive at their first audit fully prepared and equipped. This section offers practical suggestions as to how they should organise various aspects of the audit and what they should bring along with them.

5.1 Layout of Interview Room

This paragraph applies to both one-to-one interviews and focus groups used to assess data protection awareness among staff.

It is very bad practice for the Auditor to sit on the opposite side of a table or desk from the interviewee, as this will form both a physical and psychological barrier that will increase the sense of formality. It is better to provide chairs of equal appearance and height set at right angles to each other with a low table positioned between them that can be used for placing refreshments and papers.

This arrangement allows the interviewee to look away while thinking or talking and avoids the formality of the two parties having to face each other directly. Sitting too close may cause discomfort because it will be an intrusion into the interviewee's personal space, while too far away will increase the sense of formality.

Finally, both the Auditor and interviewee should avoid sitting directly in front of a window or bright light source as this will be distracting and make it difficult to see facial expressions.

5.2 Note Taking

It will nearly always be necessary to record certain key points during an interview or focus group, however, it is important not to make copious notes at the time as this will tend to inhibit the flow of the interview and make the member of staff more anxious. Detailed notes should be produced immediately after the discussions while the points are still fresh in the Auditor's mind, and the special forms of Annex D.4 have been designed for this purpose. Of course, if there are two Auditors available to conduct a focus group then one can take notes while the other leads the discussions.

As far as making notes on checklists during the audit, these will have to be done at the time to ensure that all the details are recorded accurately. There is further guidance provided on this aspect of note taking in section of 3.3.1 b) Part 3.

5.3 What to Take to the Audit

Make sure you have the following with you before starting the Audit:

- Completed Pre-Audit Questionnaire
- Completed Audit Plan
- The Audit Management Checklist
- Your completed Compliance Audit Checklists
- Copies of the relevant Procedures to be audited during the Process Audit
- Pen and paper
- Something to write on, e.g. a clipboard, as you will not always have the luxury of being at a desk or table during the audit
- Quantity of blank pro formas, i.e.:
    - Process Audit Checklists
    - Interview/Focus Group Record sheets
    - Non-compliance Record sheets
    - Observation Notes
    - Compliance Audit Report Forms

5.4 Auditor's Code of Conduct

Third party Auditors and consultants who undertake data protection audits are likely to belong to a professional auditing body such as the Institute of Internal Auditors, the International Register of Certificated Auditors or the Information Systems Audit and Control Association. In this case they will be bound by the Code of Professional Conduct of each particular body. Those who are new to data protection auditing are unlikely to belong to a professional body and so we have produced a simple Code of Conduct for their use.

5.4.1 Honesty

Auditors shall carry out their duties with honesty and diligence, and be objective and unbiased in making their judgements.

Auditors shall be loyal to their own organisation or any client for whom they are providing a service. However, they shall not knowingly be a party to any illegal or improper activity.

5.4.2 Conflict of Interest

Auditors shall not enter into any activity which may be in conflict with the best interests of their own organisation or a third party, or which would prevent them from performing their duties in an objective manner.

For example, third party Auditors should not conduct audits for a client where they have been involved in the design and implementation of the data protection system.

5.4.3 Inducements

Auditors must not accept anything of value from any member of an organisation for whom they are providing a service, which might be deemed to impair the objectivity of their judgement.

In practice, this means that it would be acceptable for an audit team to be provided with coffee and biscuits for refreshment during the audit and a sandwich lunch on the premises. However, it would not be acceptable to be taken out to a restaurant for a three-course meal. Equally it would be acceptable to be provided with pens and writing pads by the organisation but not for example with a desk diary or attaché case.

5.4.4 Confidentiality

Auditors must maintain the confidentiality of any information discovered during the course of an audit. They must not use confidential information for personal gain or in any way that would be either illegal or against the best interests of any organisation to whom they are providing a service.

5.4.5 Concealment

When producing their Audit Reports, Auditors must reveal all material facts discovered during the audit. In particular, they must reveal those facts that could distort the truth about the data protection system or conceal unlawful practices if not disclosed.

5.4.5 Professionalism

Auditors must maintain high standards of conduct and character in their professional activities and in particular:

- Auditors must not undertake work for which they do not possess the necessary technical and professional competence.

- Auditors should maintain their competency in the fields of data protection and auditing by undertaking regular professional development activities.

Annexes

Annex A: Risk Assessment

This involves first breaking down the organisation into a number of distinct areas, each of which is capable of being audited as a distinct entity. These areas would typically correspond with individual departments, functions or processes within an organisation.

Once these areas have been identified a basic risk assessment needs to be carried out for each one. The results of this risk assessment can then be used to determine audit priorities and help judge how often each of the areas needs to be audited. A straightforward approach to assessing risk is described in the following sections.

A.1 The Components of Risk

We can consider the risk of there being a breach of the Data Protection System in each area as being made up of three separate components. Each component can then be assessed and scored using the scheme suggested below:

A.1.1 Likelihood of Occurrence

What is the likelihood of a breach of the Data Protection System occurring in this area?

Score: High likelihood = 4; medium likelihood = 2; low likelihood = 1.

A.1.2 Impact

How would a breach of the Data Protection System in this area affect:

- the individual data subject?
- the data controller, managers and other staff in the short and long-term?

Score: Major impact = 4; significant impact = 2; little impact = 1.

A.1.3 Controls

How well can it be demonstrated that the Data Protection System in this area has been designed to minimise the impact of a failure on the organisation?

Score: Poorly designed = 4; moderately well designed = 2; robustly designed = 1.

A.2 Scoring the Risk

The overall risk for each area can now be calculated by multiplying together the individual scores given for Likelihood of Occurrence, Impact and Controls to arrive at a number between 1 and 64.

This final score can then be used to determine the relative priority. Judgements as to the frequency with which each area should be audited are also helped by examining the assessed risk

A.3 Other Factors

Once the basic risk has been assessed for each area of the organisation there may be other factors that could affect the audit frequency calculated in section 1.1.2. Typical factors that would influence the frequency of audits carried out in an area processing personal data would include:

- The area is directly customer facing and is vitally important to the delivery of the organisation's core business.
- Previous Audits have showed up a marked weakness in the Data Protection System in the area.
- The Data Protection System has been implemented very recently in the area.
- There have been recent or impending changes to the Data Protection System in the area.
- New staff have been introduced very recently to the area.

Annex B: Sampling Criteria

When conducting an audit, the Auditor will often be required to examine a batch of records from manual or computer files to check that they have been processed correctly and in accordance with procedures. Where there are many records involved it will often not be feasible to examine every single one from the batch, so instead we adopt the principle of taking a sample. If the records in the sample are correct then we infer that the entire batch is satisfactory, and equally, if the sample contains unsatisfactory records then we infer that the entire batch is also unsatisfactory.

The effectiveness of this type of sampling depends upon two main factors:

- Making sure that the sample size is suitable so that it is reasonable to assume that the characteristics of the sample reflect the characteristics of the entire batch.

- Making sure that the characteristics being checked are the correct ones, which implies that a certain amount of planning should be done before the sampling takes place.

The way that sample sizes are calculated for different batch sizes involves the use of probability distributions and applied statistics which is beyond the scope of this Manual. In practice it is not necessary for the Auditor to have this level of mathematical understanding as suitable sampling tables are available in textbooks and have been published as National and International Standards such as ISO 2859.

A typical sampling plan recommended for general use has been extracted from ISO 2859 and is shown in the table below which has the following features:

- This table assumes that the acceptable level of non-conforming records in the batch is 4%, i.e. a maximum of 4 out of every 100 records may contain errors. (Auditors who wish to use sampling plans with error rates different from 4% are advised to refer to ISO 2859-1:1989.)

- The first column gives the batch size and the second column specifies the corresponding number of samples that should be examined.

- If the number of faulty records in the sample equals or exceeds the number in the third column then the entire batch will have an error rate greater than 4% and will not be acceptable.

Number of records in batch	Sample size	Reject number
2 – 8	2	1
9 – 15	3	1
16 – 25	5	1
26 – 50	8	1
51 – 90	13	2
91 – 150	20	3
151 – 280	32	4
281 – 500	50	6
501 – 1,200	80	8
1,201 – 3,200	125	11
3,201 – 10,000	200	15
10,001 – 35,000	315	22
35,001 – 150,000	500	22
150,001 – 500,000	800	22
500,001 and over	1,250	22

Annex C: Audit Pro formas

This annex contains examples of all the Audit pro formas mentioned in Part 3 of the Audit Manual that are used by the Information Commissioner's own staff when carrying out Data Protection Audits. By placing these documents in the public domain the Commissioner hopes that organisations adopt them as models thus saving time and effort in designing forms for themselves.

These Audit pro formas will be of particular interest to those organisations setting up their own internal audit programmes. Of course, the pro formas included here are not meant to be rigidly prescriptive but are intended to illustrate the key elements that need to be covered. Ultimately, these pro formas are templates for organisations to adapt to the exact style and content that best suits their own needs.

IC	INTERNAL AUDIT SCHEDULE										Sheet of sheets		
Year: 2000	**DATA PROTECTION AUDIT PROGRAMME**												
Department or Function	**Audit Freq.**	**Jan**	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**

IC	PRE-AUDIT QUESTIONNAIRE		Audit Reference	
Name of Organisation				
Department				
Address				
Postcode		**Telephone**		
Fax		**E-mail**		
Contact Name				
Position/Job Title				
Products and/or services provided				
Number of sites/ locations to be covered				
Number of full-time staf		**Number of part-time staff/sub-contractors**		

DATA PROTECTION QUESTIONS

Question 1	Does your organisation process personal data on individuals?
Question 2	What personal information are collected? E.g. name, address, telephone number etc.
Question 3	Why do you hold this personal data?
Question 4	Please provide details of databases/filing systems containing personal data:

IC	PRE-AUDIT QUESTIONNAIRE	Audit Reference	

DATA PROTECTION QUESTIONS

Question 5	Do you hold any sensitive personal information (e.g. medical/health data, ethnic origin etc.)? If so, for what purpose?
Question 6	How are thess personal data collected?
Question 7	Who are these personal data collected from?
Question 8	Once personal data have been collected, do you disclose these data to anyone? (If the answer is yes, please provide examples and reasons):
Question 9	How does your organisation store personal information? E.g. on computer or manual files or both.
Question 10	Who has access to this information?

Completed by		**Date**	

IC	AUDIT MANAGEMENT CHECKLIST	Audit Reference	
Name of Organisation:			

PREPARATORY MEETING

Names of participants:			
Questionnaire completed?	☐ Yes ☐ No	**Meeting Date:**	

ADEQUACY AUDIT

Date data received:		**Date audit completed:**	
Documentation received	☐ DP Policy ☐ Procedures ☐ Codes of practice ☐ Other		
Audit outcome:	☐ Satisfactory ☐ Unsatisfactory		
Compliance Audit scheduled?	☐ Yes ☐ No	**Scheduled Compliance Audit date:**	

COMPLIANCE AUDIT

Actual Audit date:		**Audit duration (days):**	
Audit Team Leader			
Audit Team Members			

Documentation check before leaving for the audit:

☐ Pre-Audit Questionnaire ☐ Audit Plan
☐ System Audit Checklists ☐ Process Audit Checklists
☐ Interview/Focus Group Record Sheets ☐ Non-compliance Records
☐ Observation Notes ☐ Compliance Audit Reports

Names of participants at the Opening Meeting:			
Number of Major Non-compliances raised:		**Number of Minor Non-compliances raised:**	
Number of Observations made:		**Number of staff One-to-One interviews held:**	
Number of staff Focus Groups held:		**Compliance Audit Report completed?**	☐ Yes ☐ No
Names of participants at the Closing Meeting:			

IC	AUDIT MANAGEMENT CHECKLIST	Audit Reference	
Name of Organisation:			

AUDIT FOLLOW-UP

Audit Follow-up scheduled?	☐ Yes ☐ No	**Scheduled Audit Follow-up date:**	
Audit Team Leader			
Audit Team Members			
All Major Non-compliances cleared?	☐ Yes ☐ No	**All Minor Non-compliances cleared?**	☐ Yes ☐ No
Audit closed?	☐ Yes ☐ No	**Audit completion date:**	

NOTES

Completed by		**Date**	

IC	ADEQUACY AUDIT REPORT	Audit Reference	
Organisation			
Department		**Adequacy Audit Date**	

DOCUMENTATION REVIEW SUMMARY

NON-COMPLIANCES AND/OR POINTS TO BE CLARIFIED

Document reference	Item for clarification

AUDIT OUTCOME

☐ **Satisfactory:** Organisation can proceed with Compliance Audit without further action.

☐ **Unsatisfactory:** Organisation can only proceed with Compliance Audit after the above points have been clarified.

☐ **Unsatisfactory:** Compliance Audit not appropriate with current status of organisation's Data Protection System.

PROPOSED COMPLIANCE AUDIT

Estimated Compliance audit duration:	days	Estimated number of Auditors required:	
Proposed Compliance audit date:			

DP AUDITOR NAME:	SIGNATURE:	DATE:

IC	AUDIT PLAN	Audit Reference	
Organisation		Page	
Department		Audit Date	

Date	Time	Area/Function	Auditor	Activity/DP Issue Assessed

AUDIT PLAN COMPILED BY:	SIGNATURE:	DATE:

IC	NON-COMPLIANCE RECORD	Audit Reference	
Organisation		NC Reference	
Department		Audit Date	

DETAILS OF NON-COMPLIANCE

Non-compliance Category	DP Auditor Name	Signature	Date
☐ Minor ☐ Major			

CORRECTIVE ACTION PROGRAMME

Function	Signature	Date
DP Auditor		
DP Representative		
Follow-up Date		

CORRECTIVE ACTION FOLLOW-UP

Function	Signature	Date
DP Auditor		
DP Representative		

IC	OBSERVATION NOTE	Audit Reference	
Organisation		Obs. Reference	
Department		Audit Date	

DETAILS OF OBSERVATION

DP Auditor Name	Signature	Date

FOLLOW-UP ACTION (If relevant)

Function	Signature	Date
DP Auditor		
DP Representative		
Follow-up Date		

IC	COMPLIANCE AUDIT REPORT	Audit Reference	
Organisation		Page	1
Department		Audit Date	

AUDIT SUMMARY

	Function	Signature	Date
	DP Auditor		

IC	COMPLIANCE AUDIT REPORT	Audit Reference	
Organisation		Page	2
Department		Audit Date	

SUMMARY OF OBSERVATIONS

Obs. Ref.	Details of Observation

SUMMARY OF AGREED CORRECTIVE ACTIONS

NC Ref.	Action by	Corrective action to be taken	Date

AGREED AUDIT FOLLOW-UP

	Function	Signature	Date
	DP Auditor		
	DP Representative		

AUDIT CLOSED

	DP Auditor		
	DP Representative		

Annex D.1: Preparatory Meeting Agenda

1. Introductions

- Meet the data protection personnel and senior management of the organisation (if possible).
- Establish who is the key Data Protection contact within the organisation for liaison purposes before, during and after the audit.

2. Data Processing Activities

It is vital to establish from the outset what aspects of the organisation's activities come under the scope of the Data Protection Act. The questions that need to be asked are:

- Who is the Data Controller?
- Is the organisation involved in processing personal data?
- Is any of this personal data also sensitive?
- Does the organisation use any paper records which would fall within the definition of a "relevant filing system"?
- Are there any special purposes for which the data is used? E.g. journalistic, in-house newsletter etc.

3. Adequacy Audit

- Discuss what documentation the organisation should send in advance for the auditor(s) to conduct the Adequacy Audit and when it will be available.
- Outline the options open to the organisation in the event of an unsatisfactory Adequacy Audit.

4. Scope of the Compliance Audit

Once the existence of personal data processing has been established you can go on to discuss the scope of the compliance audit in more detail:

- Discuss what departments and/or functions will be involved.
- Discuss when the Audit could start and indicate the likely duration.
- Indicate which staff within the organisation are likely to be involved in the audit.

5. Compliance Audit Protocols

- Agree when and where the Opening and Closing Meetings will take place and who will be present.
- Discuss the likely schedule for the auditor(s) visiting the departments/functions and which members of staff will be involved at each stage.
- Inform the organisation of what type of written/oral feedback will be presented after the Audit, i.e. Compliance Audit Report with associated Non-compliance Reports.
- Discuss the arrangements for any potential follow-up audits/visits to confirm that any required corrective action has been taken.

6. Practical Arrangements

It is important to establish exactly which facilities will be required by the Auditor(s) during the Audit including:

- Access to premises
- Base room/office availability
- Working space, desks, furniture etc.
- Access to IT equipment
- Access to telephones, photocopiers, shredders etc.

7. Tour of the Premises

It is always good practice for Auditors to carry out a brief tour of the premises at the end of the Preparatory Meeting. This will help them to:

- Familiarise themselves with the layout of the building(s) and the nature of the organisation's products and services.
- Ascertain the status of the organisation's Data Protection System and judge how well it is prepared for an Audit.
- Prepare an initial Audit Plan, e.g. size of Audit team, skills required, likely duration.

Annex D.2: Opening Meeting Agenda

The purpose of the opening meeting is for the auditor(s) to meet the organisation's senior staff involved in Data Protection and confirm the details of the Compliance Audit as originally discussed at the Preparatory Meeting. It is recommended that the following outline agenda is used for conducting this meeting:

1. Introductions

2. Scope of the Audit

- Confirm which departments and/or functions will be involved in the Audit
- Confirm which members of staff within the organisation will be involved in the Audit and any associated Data Protection Awareness Interviews and/or Focus Groups.

3. Audit Protocol

- Confirm the schedule for the auditor(s) visiting the departments/functions and which members of staff will be involved at each stage, i.e. supply a copy of the Audit Plan.
- Confirm the time and location of the Closing Meeting and establish who will be present.
- Confirm the format of written/oral feedback that will be presented at the Closing Meeting, i.e. Compliance Audit Report with associated Non-compliance Reports.
- Discuss the arrangements for any potential follow-up audits/visits to confirm that any required corrective action has been taken.

4. Practical Arrangements

- Confirm the availability of a base room for the Auditor(s).
- Check on the facilities available in the base room.

Annex D.3: Closing Meeting Agenda

The purpose of this final meeting is for the Auditor(s) to present their findings to the organisation's key data protection staff and agree any required programme of corrective action. It is recommended that the following outline agenda is used for conducting the Closing Meeting:

1. Introductions

- Thank the organisation for their assistance, co-operation and hospitality
- Deal with any issues of confidentiality
- Emphasise that the auditing process can only sample the Data Protection System at a particular moment in time
- Ask the management team to defer any questions until after the findings have been presented

2. Presentation of Findings

- Presentation of the detailed findings which involves:
    - Confirmation of each non-compliance found
    - Agreement to suitable corrective action for each non-compliance
    - Indication of timescales for completion of corrective action
- Ask other members of the Audit Team to report if appropriate
- Presentation of an Audit summary including a judgement of the level of Data Protection compliance achieved by the organisation
- Invite questions for clarification and provide immediate answers wherever possible

3. Post Audit Reporting

- Explain to the management team the nature of summary report they will receive, e.g. Compliance Audit Report together with associated Non-compliance Reports etc.
- Establish the organisation's requirements for distribution of the summary report

4. Audit Follow-up

- Agree the nature of any required follow-up visit, e.g. documentation check, partial re-audit or full re-audit
- Arranging the timescale for any required follow-up visit

IC	INTERVIEW/FOCUS GROUP RECORD SHEET	Audit Reference	
Organisation		**Page**	**1**
Department		**Interview Date/Time**	

ATTENDEES

Name	Position	Time with organisation

DETAILS OF DISCUSSION

Question 1	What can you tell me about the Data Protection Act 1998?
Question 2	Can you tell me what you would expect the term, Data Protection to mean?
Question 3	From the data you use, what would you consider as 'personal data'?
Question 4	From the data you use, what would you consider as 'sensitive personal data'?
Question 5	Can you describe your organisational/departmental policy/procedures regarding your handling/use of these types of data?
Question 6	Can you tell me how this policy/these procedures affect your own particular job?

IC	INTERVIEW/FOCUS GROUP RECORD SHEET	Audit Reference	
Organisation		**Page**	**2**
Department		**Interview Date/Time**	

DETAILS OF DISCUSSION

Question 7	Can you describe any Data Protection training/guidance you have received? (Ask to see any documentation if available e.g. staff handbook entry, DP guidelines etc)
Question 8	How do you/does your department collect personal data/sensitive personal data?
Question 9	Where is this data held/stored? E.g. filing cabinets/databases etc
Question 10	What are the sources of this data? e.g. references, application forms, marketing lists, information transferred from another department etc
Question 11	Are you authorised to make disclosures of this data within your organisation/outside your organisation? If so, please describe this process.
Question 12	Can you describe your department's security procedures: e.g.

a) How often do you change your password?

b) How are data kept secure?

c) How are personal data/sensitive personal data disposed of/destroyed?

Auditor Name		**Signature**	

IC	E: Adequacy Audit Checklists			Page	1
Organisation		Department		Date	
Aspect	E.1 Organisational and Management Issues	Auditor		Audit ref:	

Data Protection Issue	Document reference(s)	Comments	Result
E.1.1 The Data Protection System			
a) Data Protection Policy			
b) Staffing and Reporting Structures			
c) Staff Awareness & Training			
d) Planning and Implementation			
e) System Audit and Review			
E.1.2 Documentation Issues			
a) Data Protection Procedures			
b) Job Descriptions and Staff Contracts			
c) Data collection			
E.1.3 Key Business Processes			
a) Key Business Processes			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Data Protection Issue	Document reference(s)	Comments	Result
E.2.1 The First Principle			
a) Categories of Personal Data			
b) Schedule 2 - Grounds for Legitimate Processing of Personal Data			
c) Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data			
d) Obtaining personal data			
e) Lawful Processing			
f) Fair Processing			
g) Exemptions from the First Data Protection Principle			
E.2.2 The Second Principle			
a) Uses of Personal Data within the organisation			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Data Protection Issue	Document reference(s)	Comments	Result
E.2.2 The Second Principle (continued)			
b) Use of Existing Personal Data for new purposes			
c) Disclosures of Data			
E.2.3 The Third Principle			
a) Adequacy and relevance of Personal Data			
E.2.4 The Fourth Principle			
a) Accuracy of Personal Data			
b) Keeping Personal Data up-to-date			
E.2.5 The Fifth Principle			
a) Retention Policy			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Data Protection Issue	Document reference(s)	Comments	Result
E.2.5 The Fifth Principle (continued)			
b) Review and deletion of Personal Data			
E.2.6 The Sixth Principle			
a) Subject access			
b) Appropriate withholding of personal data in response to a subject access request			
c) Processing that may cause Damage or Distress			
d) Dealing with Notices served by individuals			
e) Automated Decision Taking			
f) Rectification, blocking, erasure and destruction			
g) Staff awareness			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Data Protection Issue	Document reference(s)	Comments	Result
E.2.7 The Seventh Principle			
a) Security policy			
b) Unauthorised or unlawful processing of data			
c) Ensuring reliability of Staff			
d) Destruction of Personal Data			
e) Contingency Planning - Accidental loss, destruction, damage to personal data			
E.2.8 The Eighth Principle			
a) Adequate Levels of Protection			
b) Exempt transfers			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Data Protection Issue	Document reference(s)	Comments	Result
E.3.1 Using Data Processors			
a) Choosing a Data Processor			
b) Contract Initiation			
c) Contract review			
d) Contract modifications			
e) Contract breaches			
E.3.2 Notification			
a) Notification to the Commissioner			
b) Notification Maintenance			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Data Protection Issue	Document reference(s)	Comments	Result
E.3.3 Transitional Provisions			
a) Processing Already under way determined			
b) The first and second transitional periods			

KEY: ✓ = Issue addressed adequately ? = Issue not addressed adequately × = No reference found to issue in documentation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.1 Data Protection Policy (Good Practice – Observations Only)			
a) Does the organisation have a clearly documented statement of Data Protection Policy?			
b) Does this policy specify the organisation's top-level goals and set its requirements for Data Protection in an unambiguous manner?			
c) Does this policy commit the organisation to providing the necessary resources to ensure that the goals can be achieved?			
d) Is this Data Protection Policy: • Supported by senior management? • Distributed or made available to all staff? • How often is it reviewed and under what circumstances?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.1 Data Protection Policy (Good Practice – Observations Only)			
e) Does this Data Protection Policy: • Explain why there is a need for such a document? • Specify the intentions of senior management towards data protection?			
f) Does this Data Protection Policy: • Describe the data protection staffing and reporting structures? • Describe the links to other policies and procedures e.g. Training, Data Security, Quality Assurance etc.?			
g) Does this Data Protection Policy provide internal disciplinary sanctions for failing to comply with this policy?			
Cross reference questions e), f) and g) with questions on Data Protection Principle 7.			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.2 Staffing and Reporting Structures (Good practice - Observations Only)			
a) Has the organisation put in place an effective staffing and reporting structure to enable its data protection policy to be achieved?			
b) How does this staffing and reporting structure specify the roles and responsibilities of all staff who have access to personal data?			
c) How does this staffing and reporting structure ensure effective communication of data protection issues throughout the organisation?			
d) Has the organisation identified a person who has overall responsibility for Data Protection, e.g. a Data Protection Officer or Manager			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.3 Staff Awareness & Training			
a) How does the organisation ensure that all individuals who handle personal data have the necessary data protection awareness and training?			
b) Which categories of managers and staff receive the training?			
c) What does the training involve?			
(Cross Reference with Data Protection Principle 7, Annex G.3, Reliability of Staff.)			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.4 Planning and Implementation (Good Practice - Observations Only)			
a) How does the organisation ensure that its Data Protection Policy is implemented in a planned and systematic manner?			
b) Does the organisation have some form of Data Protection Committee or Forum for handling data protection issues?			
c) If there is a Data Protection Committee: • What is its name? • Does it involve senior management? • Does it include users from all business sectors?			
d) If there is a Data Protection Committee does it have a Data Protection representative, e.g. the Data Protection Officer or Manager?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.4 Planning and Implementation (Good Practice- Observations Only)			
e) If there is a Data Protection Committee does it have representatives from other functions, e.g. auditors, legal/compliance, security, IT?			
f) If there is a Data Protection Committee: • What are its objectives? • Which issues has it discussed in the last year?			
g) If there is a Data Protection Committee: • Which policies and procedures has it reviewed over the last year? • Does it investigate breaches of data protection procedures? Any examples?			
h) If there is a Data Protection Committee: • Does it agree corrective actions and set priorities and timescales for their implementation? Any examples? • Does it keep records of its activities?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.5 System Audit and Review (Good Practice - Observations Only)			
a) Is the organisation's data protection system subject to regular audit and review and if so with what frequency?			
b) Does the organisation have a documented procedure for conducting internal Data Protection Audits?			
c) Does the organisation have auditors who have been trained to conduct internal Data Protection Audits?			
d) If the organisation does have trained auditors, are they independent of the functions audited?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.1.5 System Audit and Review (Good Practice - Observations Only)			
e) Are the results of internal Data Protection Audits documented?			
f) Are the results of internal Data Protection Audits brought to the attention of the staff responsible for correcting any non-compliances found?			
g) Are the results of internal Data Protection Audits regularly reviewed by senior management?			
h) Is there any evidence of improvements that have been made as the results of lessons learnt from internal Data Protection Audits?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.2.1 Data Protection Procedures (Good Practice- Observations Only)			
a) Has the organisation described the arrangements and processes used to implement its Data Protection Policy in the form of documented procedures?			
b) If the organisation has produced formal Data Protection procedures are they distributed to all members of staff who need to be aware of their contents?			
c) If the organisation has produced formal Data Protection procedures are they subject to regular review, e.g. via internal Data Protection Audits?			
d) If the organisation has produced formal Data Protection procedures are they managed via an existing document control system such as ISO 9000?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.2.2 Job Descriptions and Staff Contracts (Good Practice - Observations Only)			
a) Are the Data Protection Act responsibilities and duties of staff who are involved in the handling of personal data clearly defined in their Contracts and/or Conditions of Employment?			
b) Are the processes and procedures required to safeguard data protection clearly defined in the Job Descriptions of staff who handle personal data?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.2.3 Data Collection			
a) When changes are made to either current data collection forms or software, how and at what stage are they reviewed for Data Protection Act compliance prior to implementation?			
b) When new *forms* are designed for data collection purposes, how are they checked for Data Protection compliance?			
c) When procuring new *software* for data collection purposes, how is it checked for Data Protection compliance? (Cross reference with section F.3.1 c)			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.3.1 Key Business Processes			
a) How and when is the Data Protection Act taken into consideration in the design of new business processes?			
b) How and when is the Data Protection Act taken into consideration in the specification, procurement and testing of new items of *hardware* used to support these business processes?			
c) How and when is the Data Protection Act taken into consideration in the specification, design and testing of new items of *software* used to support these business processes?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
F.3.1 Key Business Processes (continued)			
d) How does the Data Protection System integrate with other key management systems within the organisation such as: • Data Security (e.g. BS 7799)? • Health and Safety (e.g. BS 8800)? • Environmental Management (e.g. ISO 14001)? • Quality Management (e.g. ISO 9000)?			
e) Does the Data Protection System integrate with other Industry Standards for Data Management? If so, which ones and how?			
f) Does the Data Protection System integrate with other appropriate codes of practice/standards? If so, which ones and how?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.1 Categories of Personal Data			
a) What type of personal data do you process? Please give examples of any sensitive data that you process.			
b) (i) Are sensitive personal data differentiated from other personal data? (ii) If so, how?			
c) If not, why not?			
c) (i) Are sensitive personal data processed differently to other personal Data Protection within the organisation? (ii) If so, how?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.2 Schedule 2 - Grounds for Legitimate Processing of Personal Data			
a) Have you identified all the categories of personal data which you are processing and how? If so, can you list them:			
b) Have you identified the purposes for which you are processing personal data and how? If so, can you list them:			
c) Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data? If so, can you list them: (Show interviewee text of Schedule 2).			
d) (i) Will you be relying on different grounds for different categories of personal data? (ii) If so, how was this assessment made?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.3 Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data			
a) Have you identified the categories of *sensitive personal data* that you are processing? If so, how? If so, can you list them:			
b) Have you identified *the purposes* for which you are processing sensitive personal data? If so, how? If so, can you list them:			
c) Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data? If so, can you list them: (Show interviewee text of Schedule 3/Orders under Sch 3 (10)).			
d) (i) Will you be relying on different grounds for different categories of sensitive personal data? (ii) If so, how was this assessment made?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.4 Obtaining consent			
a) If you are relying on the individual providing consent to the processing as grounds for satisfying Schedule 2, when and how is that consent obtained?			
b) If you are relying on the individual providing explicit consent to the processing as grounds for satisfying Schedule 3, when and how is that consent obtained?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.5 Lawful Processing			
If you are a public sector organisation: a) (Does your processing of personal data fall within your statutory powers? If so what are they and how are they identified?			
b) Has compliance with the Human Rights Act been assessed?			
All organisations: c) Do you assess whether any of the personal data that you process is held under a duty of confidentiality?			
d) If so, how is that assessment made?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.5 Lawful Processing (continued)			
e) How is that confidentiality maintained? (e.g. Instructions on disclosure or shredding)			
f) Do you assess whether your processing is subject to any other legal or regulatory duties?			
g) If so, how is that assessment made?			
h) How do you ensure that those legal duties are complied with?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.6 Fair Processing			
a) How are individuals made aware of the identity of your organisation as the data controller?			
b) When are individuals made aware of the identity of your organisation as the data controller?			
c) How are individuals made aware of how their personal data will be used?			
d) When are individuals made aware of these uses?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.6 Fair Processing (continued)			
e) How are individuals offered the opportunity to restrict processing for other purposes?			
f) When is that opportunity offered?			
g) (i) Is any other information offered to the individual regarding your organisation's processing? (ii) If so, which information?			
h) (i) How is that information provided to the individual? (ii) And when?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.6 Fair Processing (continued)			
h) Do you receive information about individuals from third parties? (Please give examples) If yes, go to Question J, if not go to G.1.7.			
i) (i) If you do receive information about individuals from third parties, how are individuals informed that the data controller is holding personal data about them? (ii) And if so, when?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.1.7 Exemptions from the First Data Protection Principle			
The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair			
a) (i) Do you provide individuals with all of this information? (ii) Is this always the case? (If yes, go to Section G.2.1) If your organisation does not provide this information to data subjects, which exemption to these provisions is being relied upon?			
b) How is that exemption identified?			
c) How is correct reliance on the exemption assessed?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.2.1 Uses of Personal Data within the organisation			
a) What are the procedures for maintaining a comprehensive and up-to-date record of use of personal data?			
b) How often is this record checked?			
c) Does the record include all equipment which can process personal data and data held in relevant filing systems?			
d) Does the record cover processing carried out on your behalf (e.g. by a Data Processing Bureau)?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.2.2 Notifying the Data Subject			
a) What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data? (Cross reference with section G.1.6 of the First Principle)			
G.2.3 Notification to the Commissioner			
See Annex H, section H.2			
G.2.4 Use of Existing Personal Data for new purposes			
a) How is the use of existing personal data for new purposes communicated to:- • the data subject, • the person responsible for Notification within the organisation, and • the Information Commissioner? b) What checks are made to ensure that further processing is not incompatible with its original purpose? `			
G.2.5 Notification Maintenance			
See Annex H, section H.2			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.2.6 Disclosures of Data			
a) Is there a departmental/organisational policy on disclosures of data within your organisation/to third parties?			
b) Has it been documented?			
c) How are staff made aware of this policy/instructed to make disclosures?			
d) How are individuals/data subjects made aware of disclosures of their personal data?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.2.6 Disclosures of Data (continued)			
e) Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed? (If no, go to Section G.3.1)			
f) If so, how do you make the assessment?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.3.1 Adequacy and relevance of Personal Data			
a) Why are you holding the personal data?			
b) How is the *adequacy* of personal data for each purpose determined? (Please give examples.)			
c) How is an assessment made as to the *relevance* (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?			
d) (i) What are the procedures for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed? (ii) How often are these procedures reviewed?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.3.1 Adequacy and relevance of Personal Data (continued)			
e) Do you have any procedures for assessing the amount and type of personal data collected for a particular purpose? If so, what are they?			
f) Are items of personal data held in every case when they are only relevant to some?			
g) If staff are allowed to enter free text, what guidance is given to ensure its relevance?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.4.1 Accuracy of Personal Data			
a) Are personal data evaluated to establish the degree of damage to both the data subject/data controller that could be caused through inaccuracy?			
b) How, and how often, are personal data checked for accuracy? Please give examples:			
c) In which circumstances is the accuracy of the personal data checked with the Data Subject? Please give examples:			
d) (i) Is the accuracy of personal data assessed at the time of collection from sources other than the data subject to whom the data relates? (ii) If so, how?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.4.1 Accuracy of Personal Data (continued)			
e) (i) Are the sources of personal data (i.e. Data Subject, Data User, or third party) identified in the record? (ii) If so, how? Please give examples. (iii) Is there any facility to record notifications received from the data subject that they believe their data to be inaccurate?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.4.2 Keeping Personal Data Up-to-Date			
a) Are personal data evaluated to establish the degree of damage to: • the data subject or • data controller that could be caused through being out of date?			
b) Are there procedures to determine when and how often personal data requires updating?			
c) Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals? (Cross-reference with Section G.3.1on the Third Principle).			
d) (i) Are data duplicated and held separately at different locations by different departments? (ii) If so, how are updates/amendments communicated to all parties with copies of the data?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.4.2 Keeping Personal Data Up-to-Date (continued)			
e) How are third parties to whom the data has been disclosed, informed of any amendments to the personal data? (This is best practice).			
f) How are complaints about inaccuracies dealt with?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.5.1 Retention Policy			
a) (i) What are the criteria for determining the retention periods of personal data? (ii) And how often are these criteria reviewed?			
b) Have the retention periods been implemented and adhered to in practice?			
c) (i) Is a record kept of the dates on which relevant personal data were created and/or obtained? (ii) Do systems include the facility to set retention periods? If so has the facility been used?			
d) Are there any statutory requirements on retention? If so, please give examples.			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.5.1 Retention Policy (continued)			
e) Are there any sector standards on retention? If so, please give examples.			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.5.2 Review and Deletion of Personal Data			
a) (i) Is there a review policy? (ii) If so, has it been documented?			
b) When it is no longer necessary to retain data which was collected for a particular purpose • How is a review made of the data to determine whether it should be deleted? • How often is the review conducted? • Whose is responsible for determining the review? • If the personal data are held on a computer, does the application include a facility to flag records for review/deletion?			
c) Are personal data reviewed at intervals to determine if: • retention in an archive is necessary or • they can be retained in an anonomised format (e.g. if kept only for historical or statistical purposes)?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.5.2 Review and Deletion of Personal Data (continued)			
d) Are there any exceptional circumstances for retaining certain data for longer than the normal period?			
e) What are they?			
f) Who makes that assessment? (Name and Job title)			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.5.3 Deletion of Personal Data			
a) What guidance is provided on deleting personal data no longer relevant when the purpose for processing ceases to exist?			
b) (i) What is your policy on how personal data are deleted/destroyed? (e.g. shredding) (ii) Is this different for sensitive personal data?			
Cross Reference with the Seventh Principle Annex G, Section G.4, Destruction of Personal Data.			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.1 Subject Access			
a) How does the organisation identify subject access requests that are received from individuals?			
b) (i) How does the organisation identify the individual making the request?			
c) (i) Does the organisation request information from the individual in order to locate the information requested? (ii) If so, how?			
d) How do you locate all personal data relevant to a request (including any appropriate 'accessible records')?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.1 Subject Access (continued)			
e) On receipt of a request, does your organisation continue to carry out routine processing of the personal data relevant to the request?			
f) If this involves amending or deleting information relevant to the request, how is this managed in relation to the individual?			
g) How is the response collated?			
h) How is the information provided to the individual?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.1 Subject Access (continued)			
i) How is the individual provided with the relevant information about your organisation's/departments' processing?			
j) Is the individual provided with a copy of the information held?			
k) If the individual consents to *only* seeing the information, how is that arranged?			
h) (i) If any of the response is not in plain language, does the organisation provide an explanation of any codes or other unintelligible information? (ii) If so, how?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.1 Subject Access (continued)			
m) Is information relating to or identifying third parties identified in the information to be provided?			
n) If third party information is identified, is it provided to the individual making the request?			
o) If not, on what grounds would the information about third parties be withheld?			
p) How does your organisation ensure that the response is provided within the statutory timeframe?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.2 Withholding of personal data in response to a subject access request			
a) (i) Are there any circumstances where your organisation would withhold personal data from a subject access request? (ii) If so, how are the grounds for doing so, identified?			
b) (i) Do you rely on a subject access exemption? (if no, then go to Section G.6.3.) (ii) If so, how is that exemption identified?			
c) (i) Is correct reliance on the exemption assessed? (ii) If so, how and by whom?			
d) If your organisation does not rely on an exemption to the subject access provisions, which provision of the Act does it rely upon to withhold subject access?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.3 Processing that may cause Damage or Distress			
a) Are there any procedures for reviewing the processing of personal data before it begins?			
b) Would the review include an assessment of how to avoid causing damage or distress to an individual?			
c) Do you take into account the possibility that damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?			
d) Do you take any steps to alert staff of possible compensation claims? Please give examples:			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.3 Processing that may cause Damage or Distress			
e) (i) Are you aware of any processing currently underway that may cause damage or distress to an individual? (ii) If so, what is it?			
f) What are the procedures, if any, for responding to a data subject notice/Court Order asking you as the Data Controller to cease or not the begin processing of personal?			
g) Do the procedures take account of the need to respond to a notice within 21 days?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.4 Right to Object			
a) What is the procedure for complying with an individual's request to prevent processing for the purposes of direct marketing or for any other reason?			
b) Are direct marketing files checked against marketing suppression lists such as the Mailing Preference, Fax and Telephone Preference Services?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.5 Automated Decision Taking			
a) Are there any decisions made affecting individuals that are based solely on processing by automatic means?			
b) If so, what is the procedure(s) for notifying an individual that an automated decision-making process has been used?			
c) What are the procedures for responding within 21 days to a data subject notice that this decision be reconsidered or be taken via other means?			
d) Do the procedures identify 'exempt decisions' (s.12 DPA)?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.6 Rectification, blocking, erasure and destruction			
a) What is the procedure for responding to a data subject's notice (in respect of accessible records) or a court order requiring: • rectification, • blocking, • erasure or destruction of personal data?			
b) What is the procedure for notifying third parties to whom the data has been disclosed of the results of a data subject's request for rectification, blocking, erasure or destruction of personal data?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.6.7 Staff Awareness			
a) How are staff instructed to recognise and respond to initial subject access requests?			
b) How are staff instructed to respond to a formal data subject notice?			
Cross reference with the Data Protection Policy, Annex F.1.3, Staff Awareness and Training			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.1 Security Policy			
a) Is there a Data Security Policy? (This must be shown to the Auditor.)			
b) If so, who/which department(s) is responsible for drafting and enforcing the Data Security Policy within the organisation?			
c) How are the potential harm to the data subject and the nature of the data assessed to decide if the policy is appropriate?			
d) Is the level of security set taking in to account the state of technological development in security products and the cost of deploying these?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.1 Security Policy (continued)			
e) (i) How often is the Data Security Policy reviewed? (ii) What are the procedures for doing so?			
f) Does the Data Security Policy specifically address data protection issues?			
g) (i) Do you adhere to BS7799 or any other security standards/codes of practice? (ii) If so, which one(s)?			
h) What are the procedures for monitoring compliance with the Data Security Policy within the organisation?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.1 Security Policy (continued)			
i) How often is compliance with the Data Security Policy assessed and by whom/which department?			
j) (i) Are there any procedures for managing non-compliance? (ii) If so, what are they?			
k) (i) Does the Data Security Policy apply to the organisation as a whole? (ii) If not, then to which departments does it not apply and why?			
l) (i) Are there any additional security policies/procedures being adhered to by individuals or departments which are not part of the overall organisational Data Security Policy? (ii) If so which individuals/departments and why?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.2 Unauthorised or unlawful processing of data			
a) (i) Does your security policy clearly identify what constitutes unlawful and unauthorised processing? (ii) If so, please tell me. If not, can you give examples.			
b) Which security measures are in place to prevent any unauthorised or unlawful processing of: • Data held in an automated format (e.g. password controlled access to PCs) • Held in a manual record (e.g. locked filing cabinets)?			
c) (i) Is there a higher degree of security to protect *sensitive* personal data from unauthorised or unlawful processing? (ii) If so, what are the procedures?			
d) What procedures are in place to detect breaches of security (remote, physical or logical)?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.3 Reliability of Staff			
a) Have staff processing personal data been made aware of the Security Policy? Cross reference with the Data Protection Policy, Annex F.1.3, Staff Awareness and Training.			
b) (i) Are staff given any security and risk management training? (ii) If so, what does the training involve?			
c) How often are staff given training on how to implement security procedures? (Write in departments to which the reply refers.)			
d) Is training documented in guidelines/staff handbook for future reference? Please give examples:			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.3 Reliability of Staff (continued)			
e) How is access to personal data restricted to authorised staff? e.g. on a need to know basis			
f) Is each department responsible for controlling access to its personal data, or is this task centralised?			
g) How is access to systems and locations restricted to authorised personnel?			
h) (i) Are staff authorised to take equipment/software for external use/to work from home (eg a laptop)? (ii) If so, do they receive any specific instructions on how personal data, which may be stored on this equipment/software, should be safeguarded? Please give examples:			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.4 Destruction of Personal Data			
a) How is the destruction of personal data that are no longer necessary carried out to prevent unauthorised access?			
b) Are there different procedures for destroying *sensitive* personal data?			
Cross Reference with the Fifth Data Protection Principle, Annex G.5.3, Deletion of Personal Data.			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.5 Contingency Planning - Accidental loss, destruction, damage to personal data			
a) Is there a contingency plan to manage the effect(s) of an unforeseen event?			
b) (i) If so, has this plan been tested? How often? (ii) Has the contingency plan been amended as a result of the test? If so, how?			
c) (i) Are staff informed of contingency procedures? (ii) If so, how often?			
d) (i) Are personal data backed-up? If so how often? e.g. on site/off site (ii) Where are the back ups held?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.7.5 Contingency Planning - Accidental loss, destruction, damage to personal data (continued)			
e) (i) Do you permit live data to be used for testing purposes? (ii) If so, what procedures are used to protect the personal data during and after testing?			
f) What are the risk management procedures, if any, to recover data (both automated and manual) which may be damaged/lost through: • human error • computer virus • network failure • theft • fire • flood • other disaster?			
G.7.6 Contracts for Processing Carried out by Third Parties			
Please refer to Annex H, Section H.1.			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.8.1 Adequate Levels of Protection			
a) Are you aware of the issues surrounding this Principle?			
b) (i) Does the organisation transfer personal data to a country or territory outside the EEA? (ii) If so, where? (If no, do not ask any other questions on this Principle.)			
c) What are the purposes for making transfers of personal data abroad?			
d) What are the types of data transferred? (e.g. contact details, employee records)			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.8.1 Adequate Levels of Protection (continued)			
e) Are any sensitive personal data transferred abroad? If so, please provide details.			
f) What are the main risks involved in the transfer of personal data to countries outside the EEA?			
g) What measures are taken to ensure an adequate level of security when the data are transferred to another country or territory?			
h) Has the organisation checked whether the non EEA state has been deemed as having adequate protection?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
G.8.2 Exempt Transfers			
a) Does the organisation carry out any transfers of data where it has been decided that the Eighth Principle does not apply?			
b) If so what are they?			
c) To which country/territory are these transfers made?			
d) What is the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle? E.g. consent, (See Schedule 4, DPA 1998, for a full list)			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.1.1 Choosing a Data Processor			
a) How does your organisation actually choose its Data Processor(s)? Does this involve choosing one providing sufficient guarantees on security?			
b) What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?			
c) How did you assess their data security measures? (eg risk assessment procedures)			
d) How do you ensure that the Data Processor complies with these measures?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.1.1 Choosing a Data Processor (continued)			
e) Is there an on-going procedure for monitoring their data security measures?			
f) How does this procedure work?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.1.2 Contract Initiation			
a) How do contracts deal with specific Data Protection and/or security issues such as: • Notification (e.g. who is the Data User)? • Limitations (e.g. on disclosures and use of data)? • Obligations to comply with any limits set? • Relevant security and data protection standards?			
b) Is there a written contact?			
c) Do existing contracts include provisions requiring the processor to only act on instructions form the organisation and comply with its security obligations?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.1.3 Contract Review			
a) How is the contract checked to ensure that all necessary requirements are specified?			
b) How are the results of any contract reviews documented?			
c) If the contractor uses any agents, how are they identified and how are their responsibilities assigned?			
d) If your organisation sets any audit requirements, how are these specified, carried out and reported?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.1.4 Contract Modifications			
a) How are modifications to contracts initiated, authorised and implemented?			
b) Who is responsible for making improvements to standards that are found to be inadequate?			
c) When a contract expires or is terminated, what are you procedures regarding personal data held? (Eg Who retains the data? What happens to it?)			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.1.5 Contract Breaches			
a) What happens in the case of breaches of Data Protection Act principles, such as security, or data controller's duties?			
b) How are indemnities specified (if any) in case of breach of contract conditions?			
c) How does the Data Processor obtain authorisation from your organisation for overseas transfers of personal data to territories outside the EEA?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.2.1 Notification to the Commissioner			
a) Who is responsible for the organisation's notification to the Commissioner?			
b) Can the person(s) responsible for Notification be identified by staff within the organisation?			
c) To what extent do the Notification entries reflect the actual processing of data?			
d) How often is this point reviewed?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.2.1 Notification to the Commissioner (continued)			
e) Are the registered purposes lawful and do they comply with any legal constraints to which the organisation is subject?			
f) Does each notification entry adequately reflect the personal data that are held?			
g) Are any exemptions from notification relied upon?			
h) If any exemption is relied upon, how is continued compliance with the terms of the exemption maintained?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.2.2 Notification Maintenance			
a) What are the procedures for keeping the Notification entry up-to-date?			
b) How are staff kept informed of how the Notification entry correspond to their work?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.3.1 Processing Already under way			
a) Has your organisation distinguished between 'processing already under way' and new processing started after October 24th 1998 to identify data which is subject to the Data Protection Act 1998? If so, how?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.3.2 Dual Regime			
a) What steps have been taken to ensure that the organisation's working practices and systems take account of personal data which are subject to the Data Protection Act *1998* and personal data which are not?			
b) Has data eligible for continuing under the terms of the Data Protection Act *1984* been clearly identified within the organisation?			
c) What guidance, if any, has been given to staff on how to operate this dual regime?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.3.3 The first and second transitional periods			
a) How are personal data added after the 24th October 1998, identified?			
b) What are the procedures for identifying personal data that may be exempt until October 24th 2001?			
c) How is the organisation preparing to incorporate Manual Data within the organisation's Data Protection system after October 24th 2001?			
d) Has the organisation prepared procedures for changing the way eligible data are processed after the first transitional period ends in 2001 and the 2nd transitional period ends in 2007?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result
H.3.3 The first and second transitional periods (continued)			
e) If so, what are these procedures?			
f) How have staff been instructed to process data once transitional relief no longer applies?			

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

IC	J: Process Audit Checklist			Page	
Organisation		Auditee		Date	
Process		Auditor		Audit ref:	

Question/Check	Evidence (Documents) Examined	Findings and Observations	Result

KEY: COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation