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:

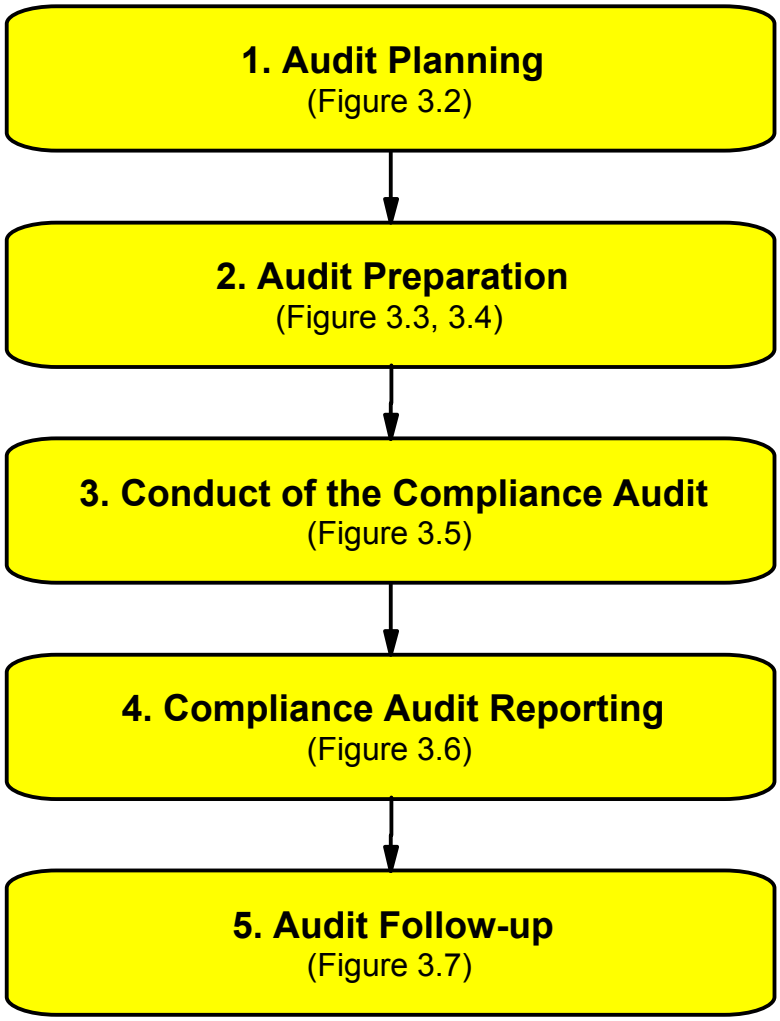

Fig. 3.1: The Data Protection Audit Lifecycle

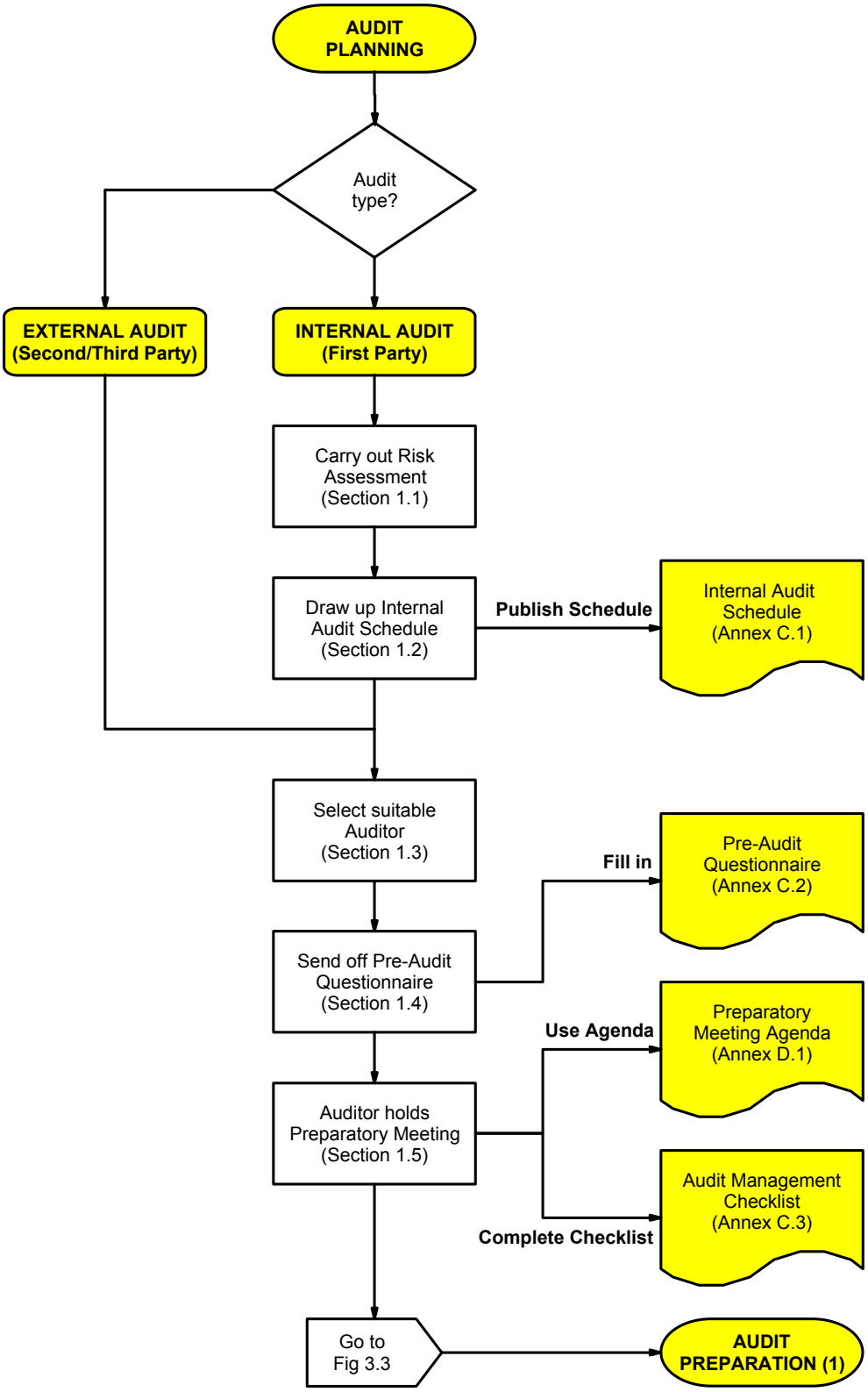

Fig. 3.2: Audit Planning

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

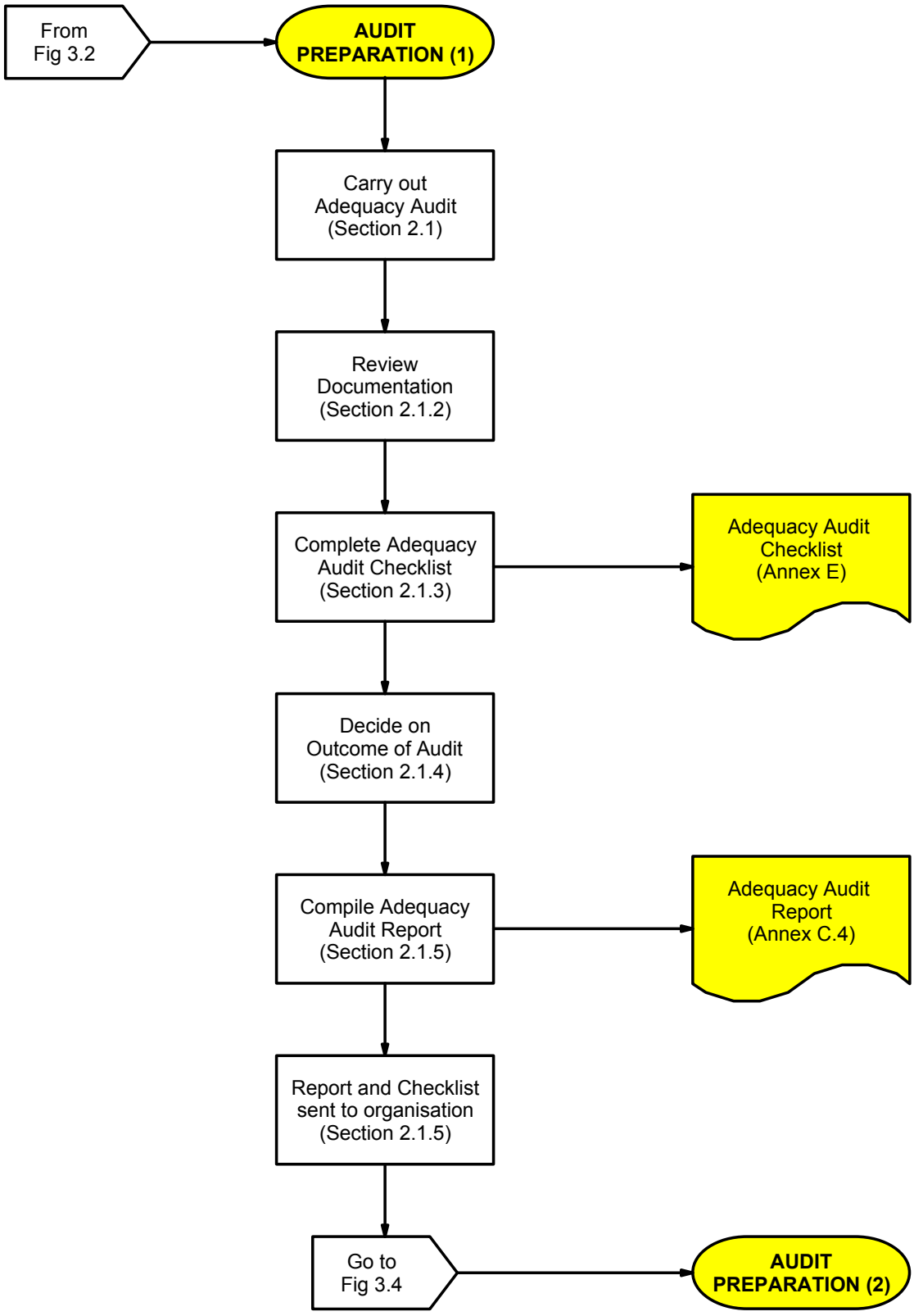

Fig. 3.3: Audit Preparation (1)

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

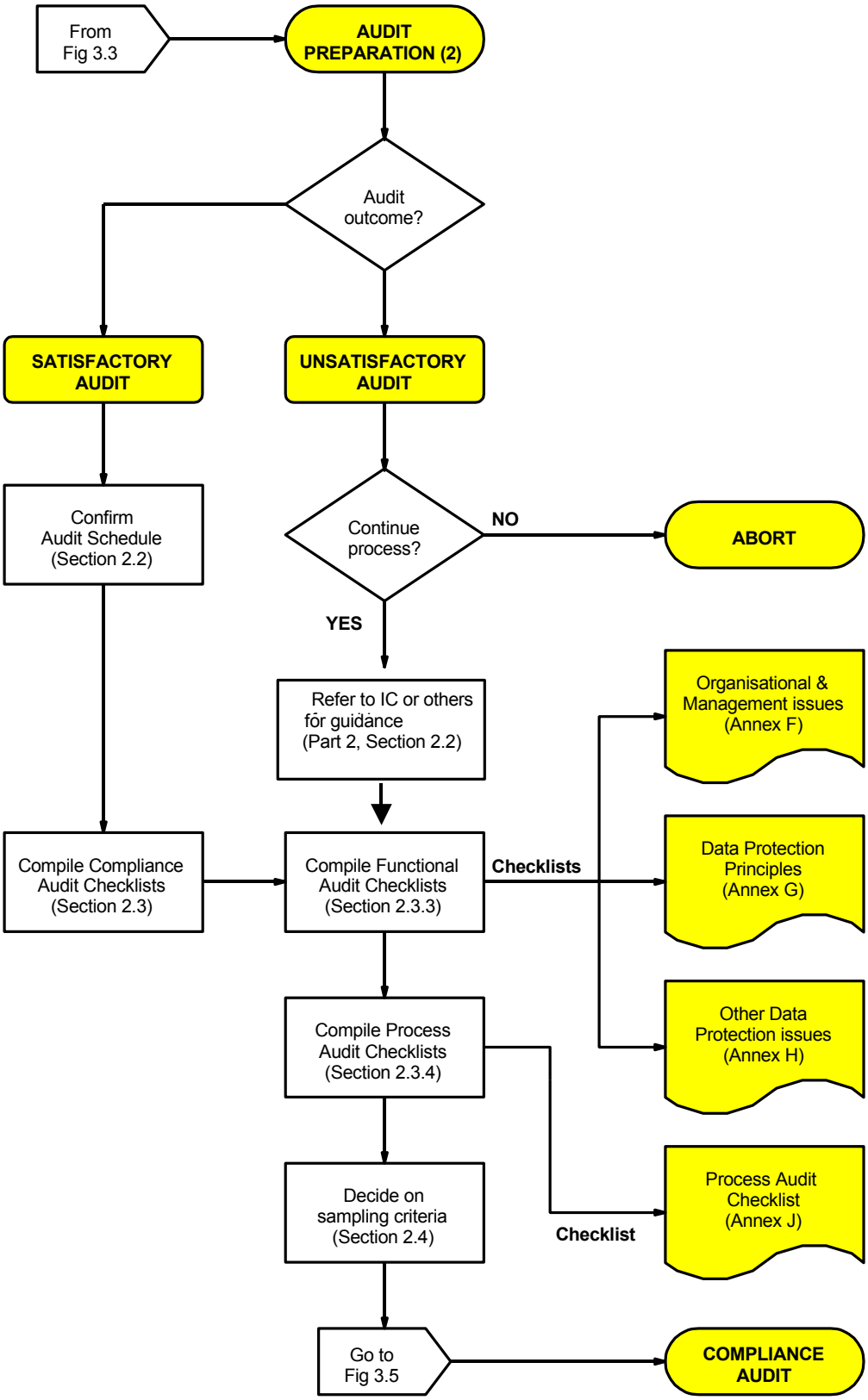

Fig. 3.4: Audit Preparation (2)

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.

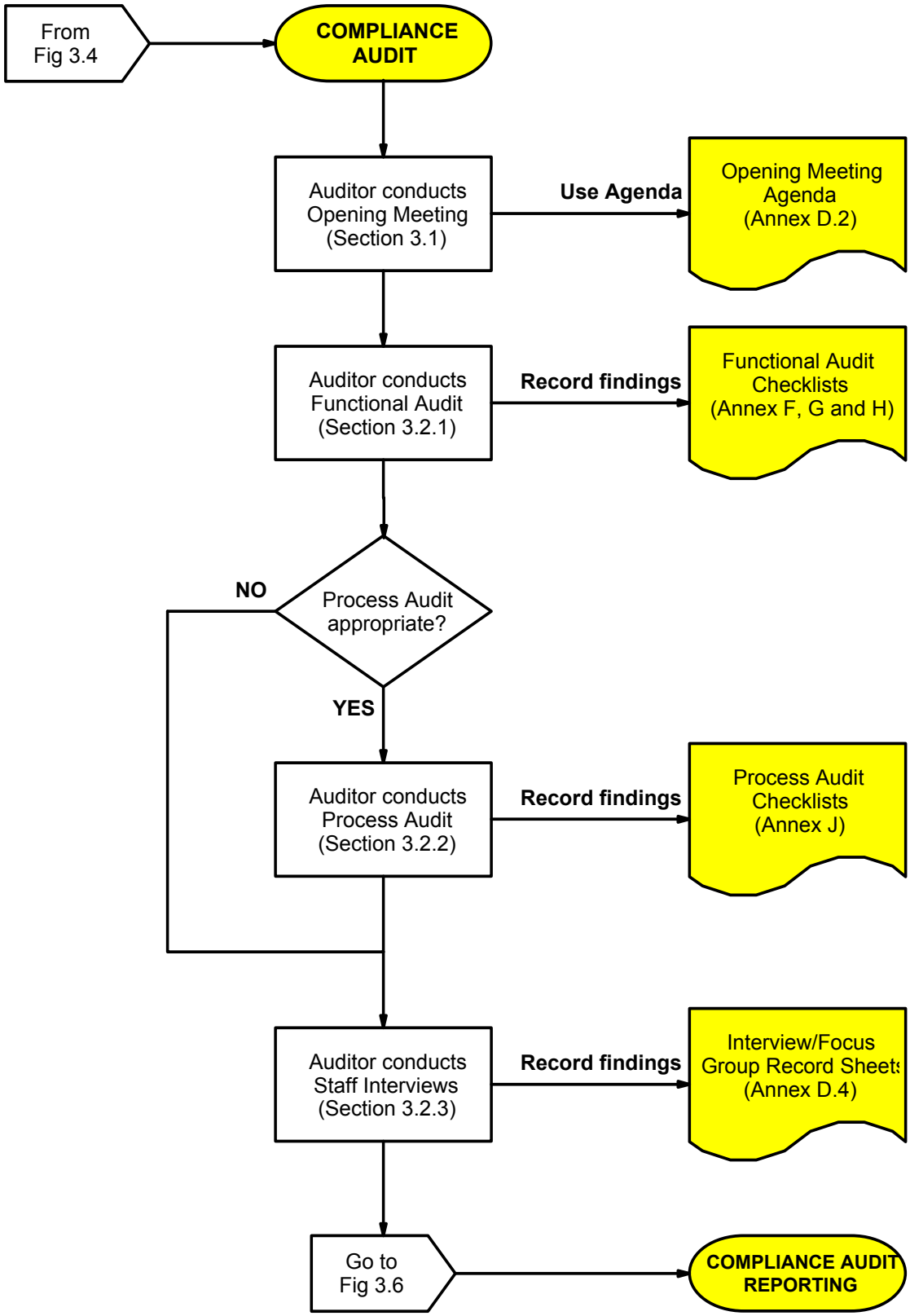

Fig. 3.5: Conduct of the Compliance Audit

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.

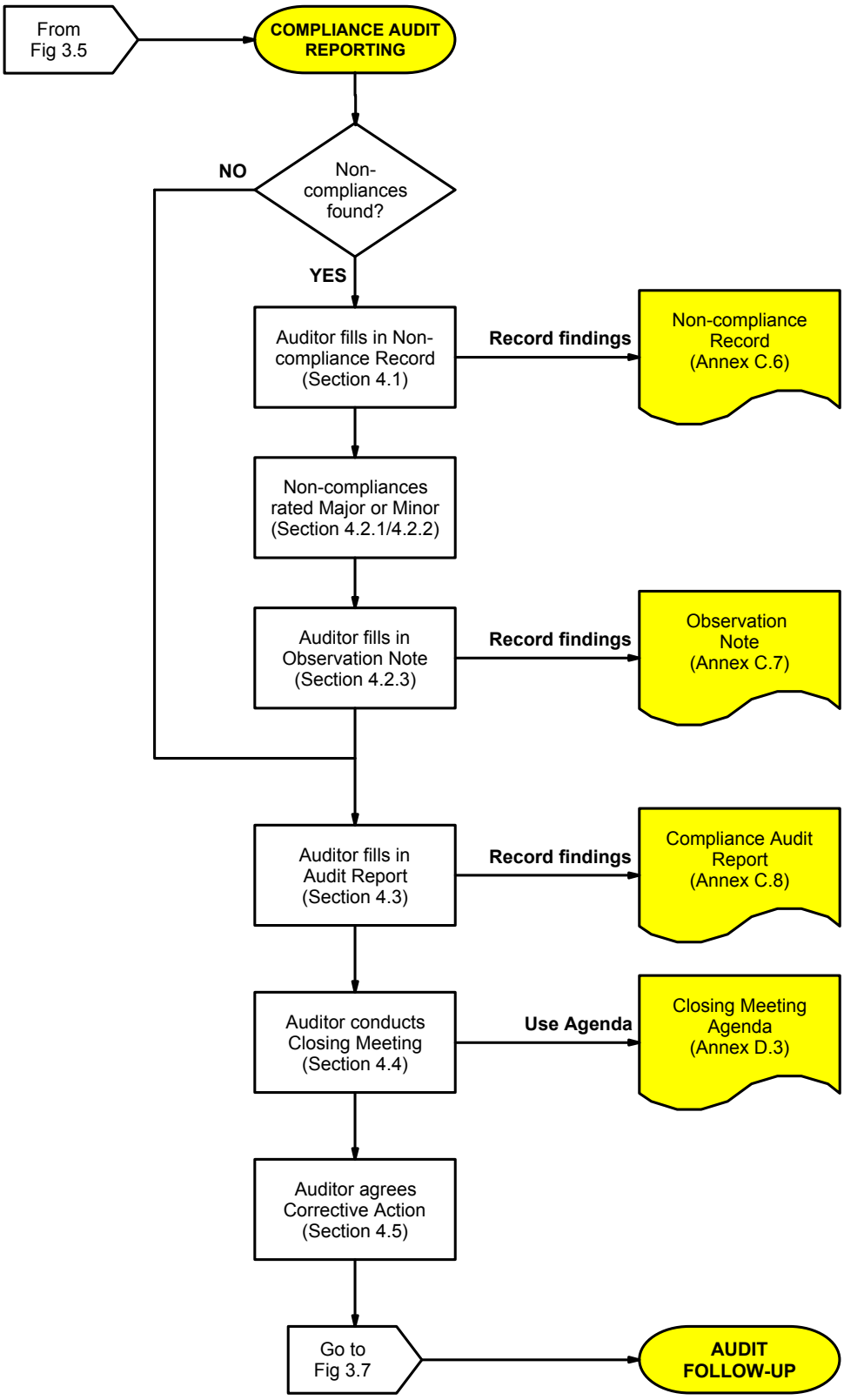

Fig. 3.6: Compliance Audit Reporting

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.

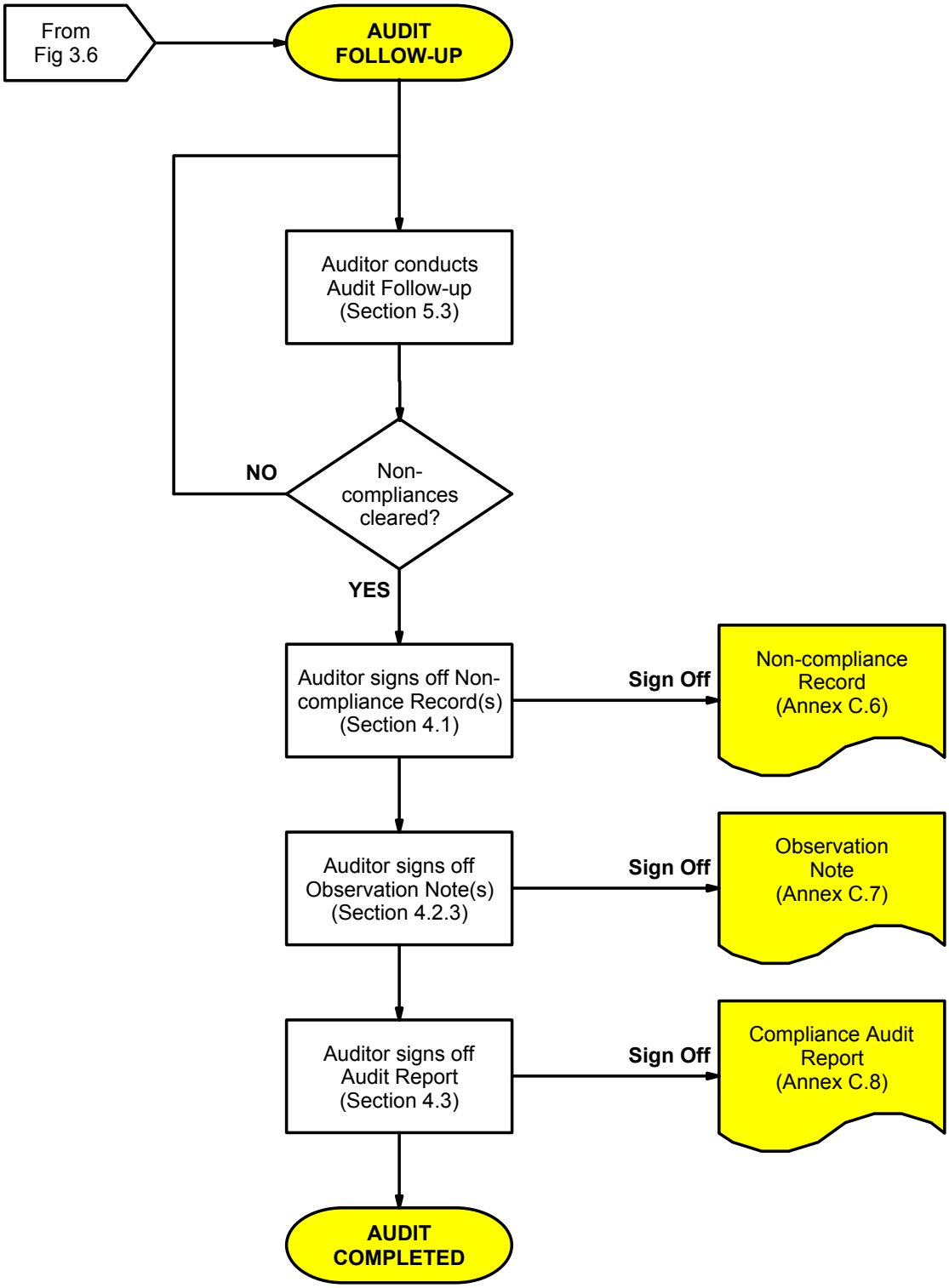

Fig. 3.7: Audit Follow-up

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.