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

_____
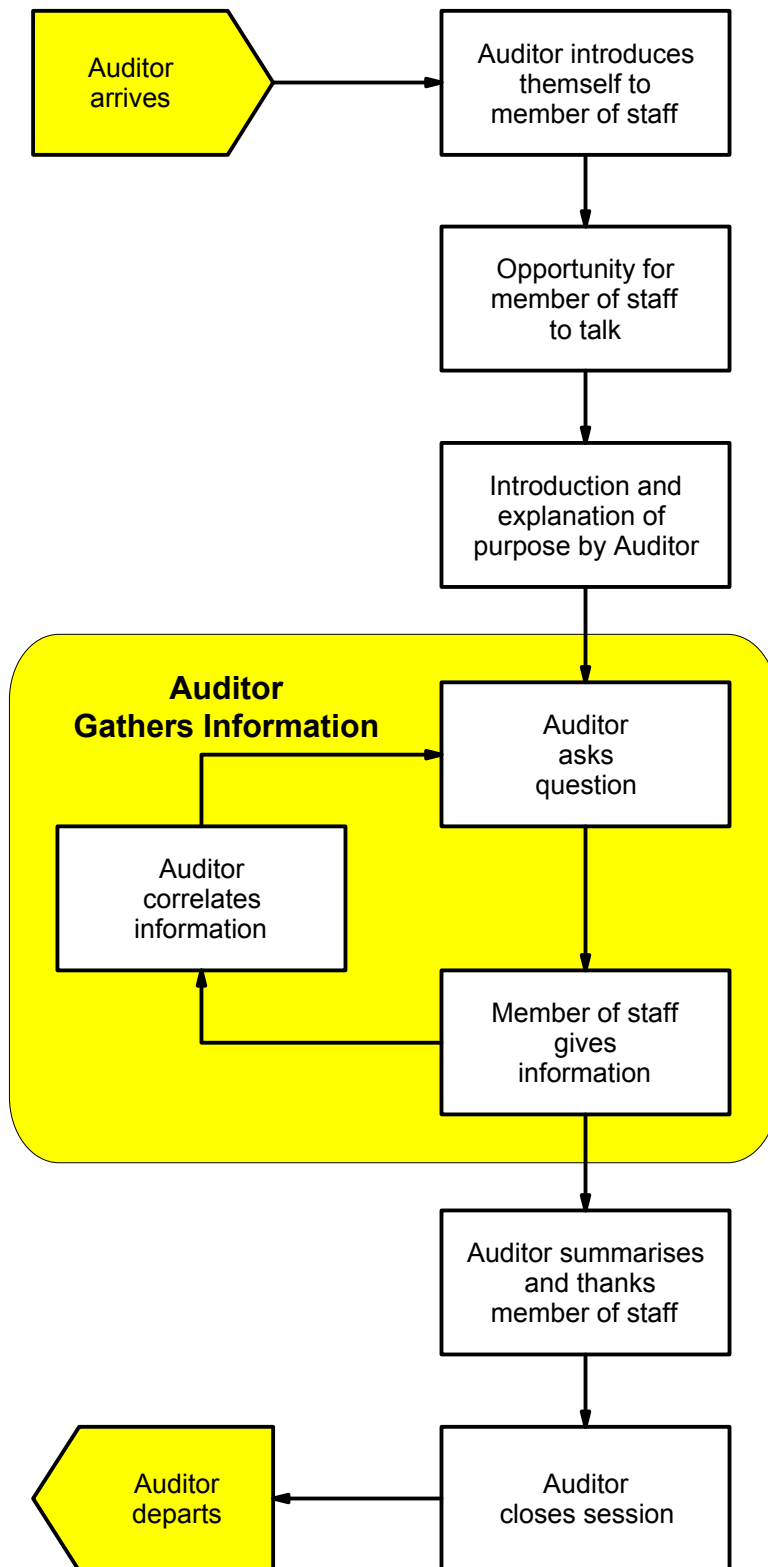
2.1 Obtaining Evidence

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?

Work and Resources		
Input checks adequate?	Training adequate?	Output checks adequate?

Process Inputs → Input checks → "Black Box" Process → Output checks → Process Outputs

Input checks → Corrective and Preventive Action ← Output checks

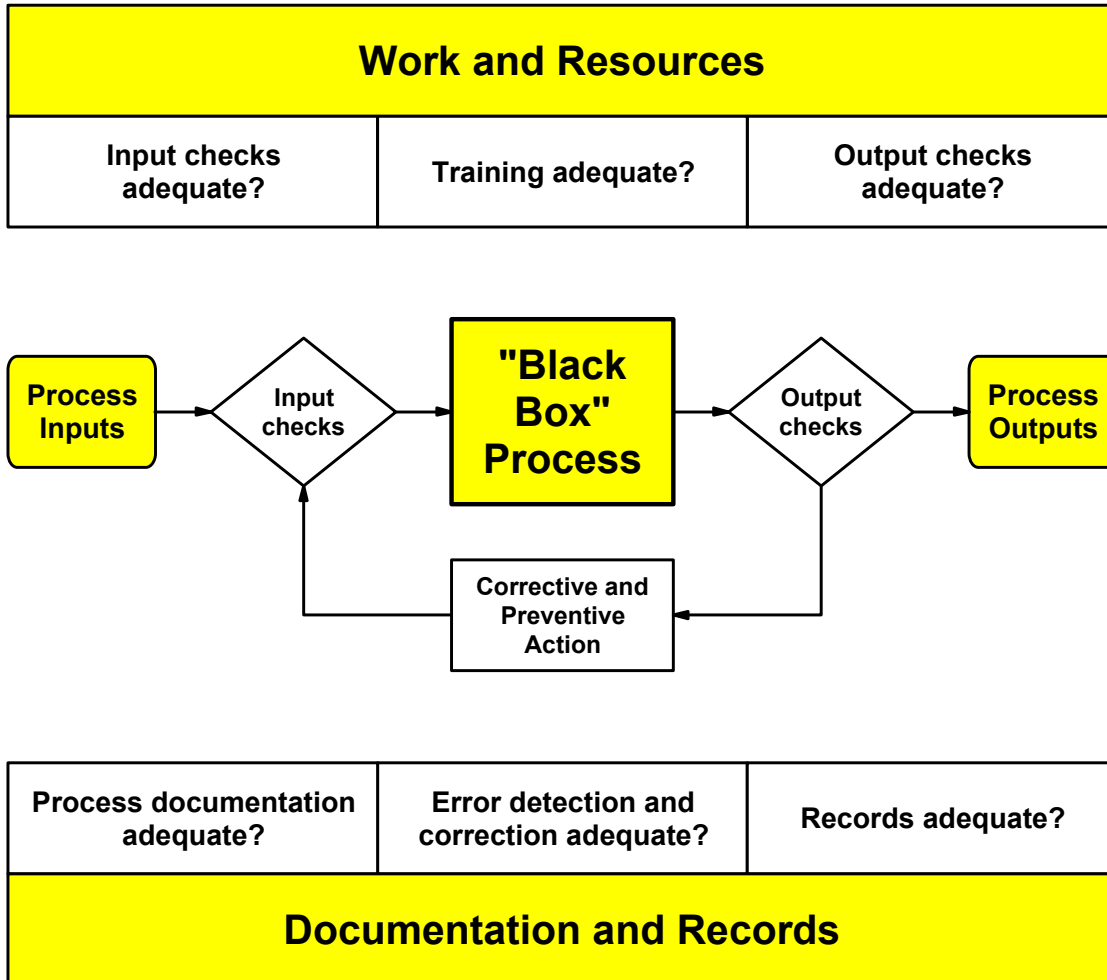| Process documentation adequate?	Error detection and correction adequate?	Records adequate?
Documentation and Records		

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.

_____