Part 2: The Audit Method

Section	Title	Page
Part 2	**The Audit Method**	**2.2**
1.	**Audit Categories**	**2.2**
1.1	Purpose of Adequacy Audits	2.3
1.2	Purpose of Compliance Audits	2.3
1.3	Audit Evidence	2.3
2.	**Adequacy Audit Outcomes**	**2.4**
2.1	Satisfactory Adequacy Audit	2.4
2.2	Unsatisfactory Adequacy Audit	2.4
3.	**Compliance Audit**	**2.4**
3.1	Functional or Vertical Audit	2.4
3.2	Process or Horizontal Audit	2.5
3.3	Interactions with Staff	2.6
3.3.1	Staff Questioning	2.6
3.3.2	Staff Awareness Interviews	2.7

Illustrations

Figure	Title	
2.1	The Three Audit Categories	2.2
2.2	Functional or Vertical Audit	2.5
2.3	Process or Horizontal Audit	2.6

Part 2: The Audit Method

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

1. Audit Categories

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

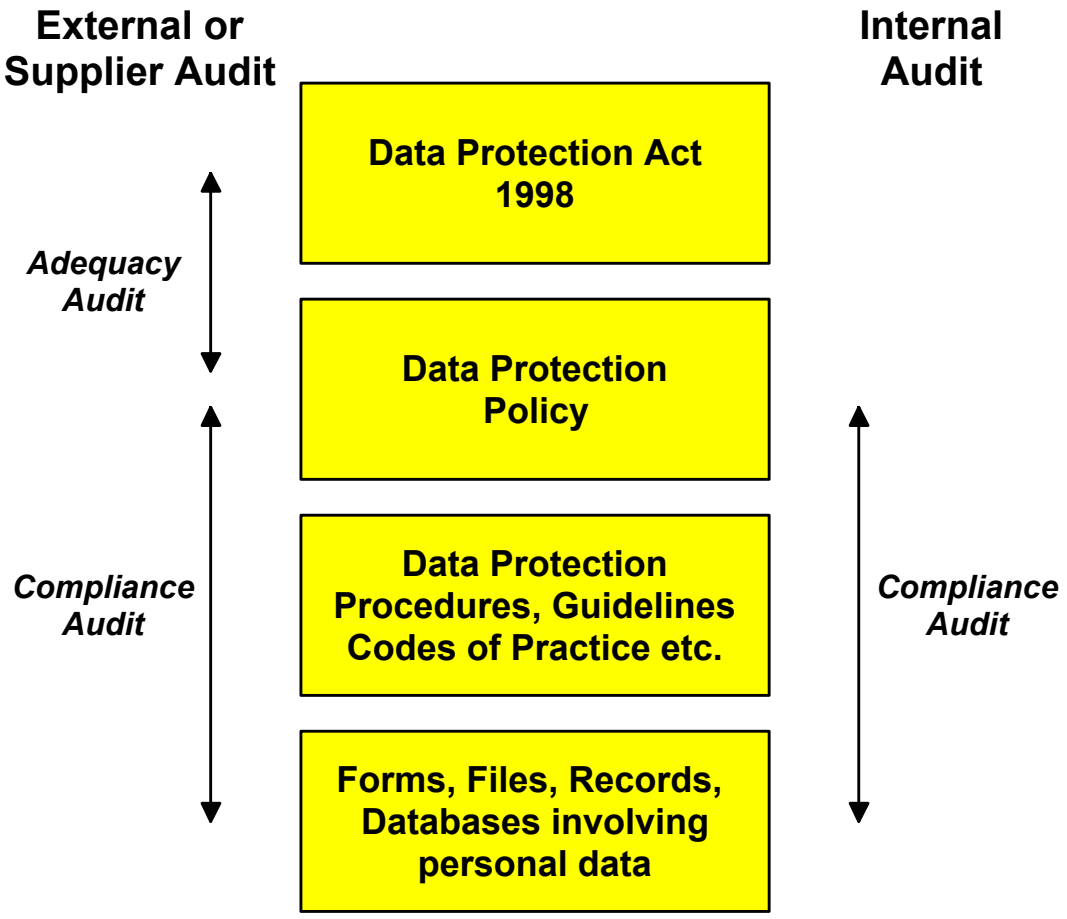

Fig. 2.1: The Three Audit Categories

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

1.1 Purpose of Adequacy Audits

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

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

1.2 Purpose of Compliance Audits

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

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

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

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

1.3 Audit Evidence

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

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

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

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

2. Adequacy Audit Outcomes

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

2.1 Satisfactory Adequacy Audit

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

2.2 Unsatisfactory Adequacy Audit

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

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

3. Compliance Audit

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

3.1 Functional or Vertical Audit

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

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

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

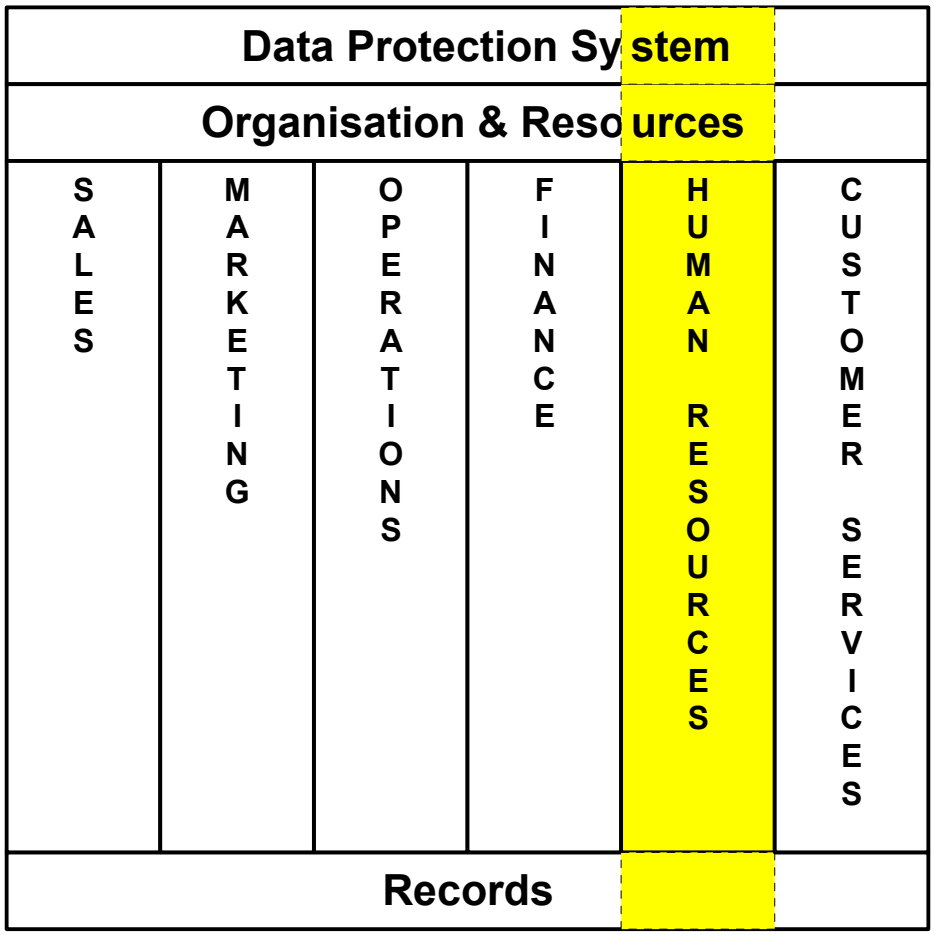

Fig. 2.2: Functional or Vertical Audit

3.2 Process or Horizontal Audit

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

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

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

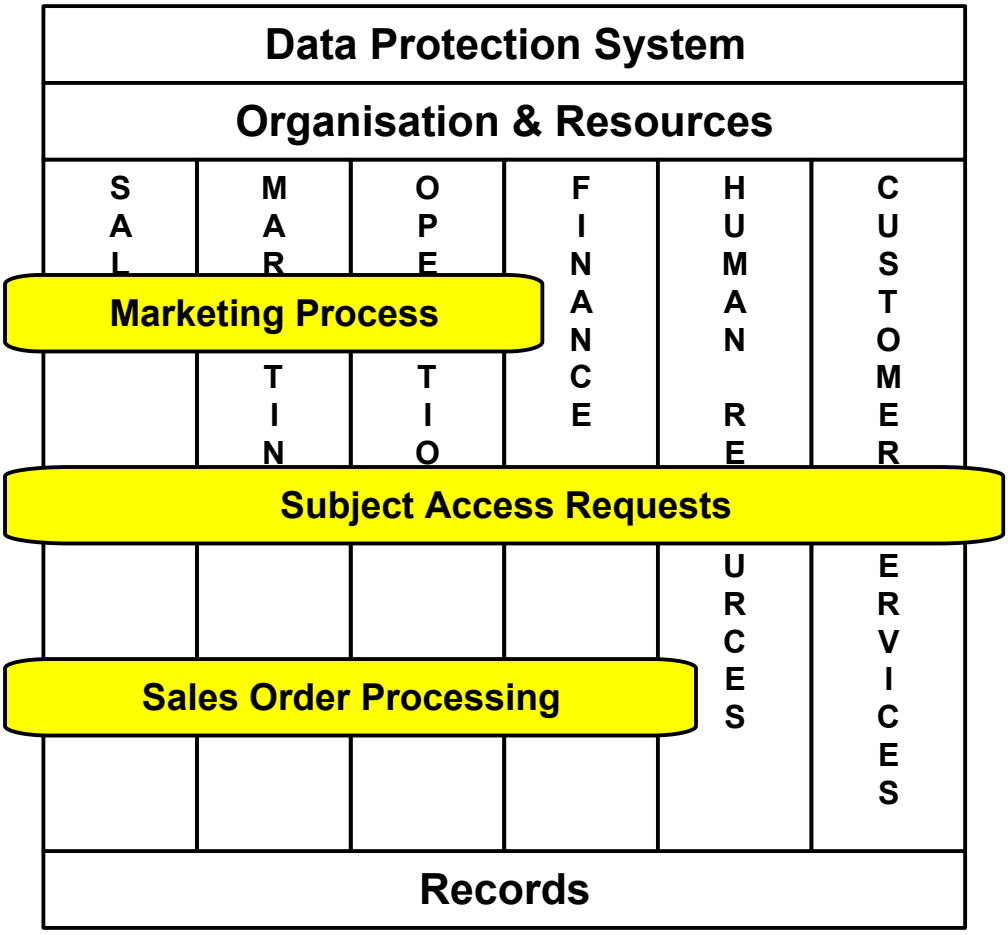

Fig. 2.3: Process or Horizontal Audit

3.3 Interactions with Staff

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

3.3.1 Staff Questioning

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

3.3.2 Staff Awareness Interviews

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

- One-to-one interviews
- Focus groups

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

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