Annexes

Annex A: Risk Assessment

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

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

A.1 The Components of Risk

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

A.1.1 Likelihood of Occurrence

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

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

A.1.2 Impact

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

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

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

A.1.3 Controls

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

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

A.2 Scoring the Risk

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

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

A.3 Other Factors

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

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