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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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