

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	1
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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: <ul style="list-style-type: none"> 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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	2
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	3
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	4
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	5
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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: <ul style="list-style-type: none"> 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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	6
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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: <ul style="list-style-type: none"> What are its objectives? Which issues has it discussed in the last year? 					
g) If there is a Data Protection Committee: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	7
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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					

IC	F: Compliance Audit Checklists: Organisational & Management Issues			Page	8
Organisation		Auditee		Date	
Aspect	F.1 The Data Protection System	Auditor		Audit ref:	
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					