CLEAR QUALITY

Summary of Gap analysis in line with 27001 standards

CLAUSE	CURRENTLY IN PLACE	REQUIRED FOR ISO 27001	ACTIONS / BY WHO
4.1 - Context of the organisation		ISMS Manual	
4.2 - Interested parties (internal and external)		Interested parties register	
4.3 – SCOPE and Certification Scope for the ISMS system		Must include any clause/subclause not required and why.	
4.4 – ISMS			
5.1 – Leadership and commitment to the ISMS		Quality policy/manual, contract review, customer feedback	
5.2 -Information Security Policy		Quality policy, visible for all to see	
5.3 – Roles & Responsibilities within the ISMS		Roles and responsibilities chart (can be included in the Quality manual)	
6.1 – RBT (Risk-based thinking) Risks and Opportunities		Change management procedure, risk treatment control, inventory of assets, Risk Treatment plan, Risk assessment. Need to verify any controls in Annex A that have been omitted. Statement of Applicability.	
6.2 – ISMS Objectives and planning to achieve them.		Within the Security Policy, be measurable: what, who, when, results, resources, how,	

Summary of Gap analysis in line with 27001 standards

7.1 – Resources		People, infrastructure, environment, monitoring and measuring. Training matrix, training logs, job descriptions, CPD, internal (knowledge from experience, completed projects, processes in place) and external (standards, conferences, external providers)	
7.2 – Competence		Training matrix, training logs, job descriptions	
7.3 – Awareness		Documentation that employees need to follow, how they contribute and what happens if they don't. CAR forms (updated training records, meeting minutes, etc)	
7.4 – Communication		What is communicated, when, with whom, how and by whom	
7.5 – Documented information		Document control procedure revision dates, reasons	
8.1 – Operation planning and control –		requirements of products or services for each customer, agreement to supply, confirmation of order, Contract review procedure	
8.2 –Information Security Risk Assessment		Linked to 6.1.2	
8.3 –Information Security Risk Treatment			

Summary of Gap analysis in line with 27001 standards

9.1 – Monitoring, measuring, analysis and evaluation		Information Security processes/controls: when, who, analyse and evaluate.	
9.2 - Internal Audits		Audit schedule, audit checklist, audit summary, procedure, NC procedure, CAR documents.	
9.3 - Management Review		MRM minutes, Agenda to cover 27001. Documented information	
10.2 -Nonconformity and corrective action		CAR system, procedure, CAR forms, CAR register. Monitoring.	
10.3 – Continual improvement		Opportunities register, internal audits, MRM minutes, QMS documents.	