ISO 27001

Action Plan

Issued 2026

Chosen UKAS Certification Body	
ISO 27001 Stage 1 Target Date	
ISO 27001 Stage 2 Target Date	

No	Action	Who	Progress / Target
1	Conduct a Gap Analysis to ISO 27001:2022. This will outline the requirements for gaining certification to ISO 27001 along with the actions listed below.		
2	Commence work on the Context of the Organisation including the following: • Internal Issues • External Issues • Interested Parties • Risks and Opportunities		
3	Develop the Scope of the Organisation		
4	Develop an Actions system for tracking actions, improvements and opportunities		
5	Issue an Information Security Manual and relevant Management Procedures. Develop a full set of Operational Processes		
6	Develop an Information Security Risk Assessment		
7	A coherent and documented Risk Treatment Plan should be established to reduce the risks outlined in 6 above		
8	Develop a Statement of Applicability using the following criteria: • 5. Organisational Controls • 6. People Controls • 7. Physical Controls • 8. Technological Controls		
9	A full ISMS Management Review should be conducted.		

No	Action	Who	Progress / Target
10	Using the Risks and Opportunities in the Context and other analysis, develop a comprehensive set of Information Security SMART Objectives.		
11	Conduct training in Information Security Management for relevant staff, including the information security awareness briefing.		
12	Develop an ISMS Internal Audit Schedule and complete the audits.		