Strike Graph

ISO 27001

ISO 27701

ISO 27001 AND ISO 27701

Certification Checklist Cheat Sheet

Scope: Define the scope of the ISMS and PIMS, and identify overlapping roles, responsibilities, and resources.

Gap analysis: Assess your current state of information security and privacy.

Risk assessment: Evaluate risks and define mitigating controls.

Statement of Applicability: Compile an SOA, noting which 27001 Annex A and 27701 Annexes A and B you include or exclude in your IS-PMS and why.

Implementation: Implement your IS-PMS. Inform internal and external users about the system.

Training: Train your team on new security policies and procedures.

Internal audit: Do your internal review.

Stage 1 audit: Your external auditor reviews documentation and interviews key personnel to ensure your organization is ready for the Stage 2 audit.

Stage 2 audit: Your auditor verifies that your IS-PMS is correctly and effectively implemented, and you incorporate feedback.

Ongoing review: You keep monitoring, assessing, and improving.