ISO 27001 COMPLIANCE CHECKLIST

A guide to building your Information Security Management System (ISMS)

1. UNDERSTAND THE STANDARD

- [ ] *Purchase and review the ISO/IEC 27001:2022 standard*
- [ ] *Obtain ISO/IEC 27002:2022 for guidance on implementing controls*
- [ ] *Understand the PDCA model (Plan-Do-Check-Act)*
- [ ] *Brief your team on ISO 27001's structure and intent*

2. DEFINE SCOPE & CONTEXT

- [ ] *Define the scope of your ISMS (systems, locations, teams, processes)*
- [ ] *Identify internal and external issues (Clause 4.1)*
- [ ] *Identify interested parties and their requirements (Clause 4.2)*
- [ ] *Document your ISMS scope (Clause 4.3)*

3. LEADERSHIP & COMMITMENT

- [ ] *Appoint top-level ISMS leadership and assign roles (Clause 5.1, 5.3)*
- [ ] *Write and approve an Information Security Policy (Clause 5.2)*
- [ ] *Ensure ISMS responsibilities are integrated into business processes*
- [ ] *Promote awareness and communicate intent from the top*

4. RISK MANAGEMENT

- [ ] *Establish a risk assessment methodology (Clause 6.1.2)*
- [ ] *Identify information assets and associated threats*
- [ ] *Assess likelihood and impact of risks Determine risk acceptance criteria*
- [ ] *Select appropriate controls (Annex A) Create a Risk Treatment Plan*
- [ ] *Complete and maintain your Statement of Applicability (SoA)*

5. REQUIRED DOCUMENTATION

- [ ] *ISMS Scope*
- [ ] *Information Security Policy*
- [ ] *Risk Assessment and Risk Treatment Methodology*
- [ ] *Risk Register*
- [ ] *Statement of Applicability*
- [ ] *Asset Inventory*
- [ ] *Roles and Responsibilities*
- [ ] *Access Control Policies*
- [ ] *Incident Response Procedure*
- [ ] *Internal Audit Program*
- [ ] *Management Review Records*
- [ ] *Corrective Action Register*

6. ANNEX A CONTROLS

- [ ] *Identify applicable controls from the 93 in ISO 27001:2022 Annex A*
- [ ] *Create implementation steps for each applicable control*
- [ ] *Use ISO 27002 as a guide for control implementation*
- [ ] *Document control owners and timelines*

7. MONITOR, AUDIT & IMPROVE

- [ ] *Create an internal audit schedule (Clause 9.2)*
- [ ] *Conduct regular audits and record findings*
- [ ] *Conduct management reviews (Clause 9.3)*
- [ ] *Implement corrective actions for nonconformities (Clause 10.1)*
- [ ] *Plan for continual improvement of the ISMS (Clause 10.2)*

8. CERTIFICATION PREP

- [ ] *Engage a reputable certification body*
- [ ] *Conduct a gap analysis*
- [ ] *Prepare for Stage 1 audit – documentation readiness*
- [ ] *Prepare for Stage 2 audit – full implementation review*
- [ ] *Maintain documentation for surveillance audits*

Pro tip: If it's not documented, it didn't happen. Your ISMS lives and dies by clear, maintained records.