ISO 27001 PDCA Audit Checklist

This checklist is designed to guide auditors and implementers through the key elements of the Plan-Do-Check-Act (PDCA) cycle as applied in ISO 27001. Use this as a practical tool to assess whether each phase is adequately addressed during implementation or auditing.

PLAN

- Has an Information Security Management System (ISMS) scope been defined?
- Have the context of the organisation and interested parties been identified?
- Are information security objectives established and documented?
- Has a risk assessment methodology been defined and applied?
- Are risk treatment plans in place and documented?
- Are resources and responsibilities clearly allocated?

DO

- Have the necessary controls been implemented based on the Statement of Applicability (SoA)?
- Is there documented evidence of communication and awareness efforts?
- Are operational procedures and processes being followed and maintained?
- Are incident management processes in place and functioning effectively?

CHECK

- Are regular internal audits being conducted?
- Is there a schedule for management reviews?
- Are key performance indicators (KPIs) or metrics in place to monitor ISMS effectiveness?
- Are nonconformities and corrective actions tracked and addressed?

ACT

- Are continual improvement actions identified and implemented?
- Are corrective actions documented, followed through, and evaluated for effectiveness?
- Is the ISMS updated to reflect changes in the business or risk environment?