TIEBREAKER Ai

ISO 27001 COMPLIANCE CHECKLIST

ISO 27001 is the leading global standard for safeguarding information and ensuring the security of critical business assets. Achieving ISO 27001 certification demonstrates to stakeholders that your organization adheres to internationally recognized security practices.

This roadmap is designed to help your organization develop and implement an effective Information Security Management System (ISMS). By following these steps, your team will be equipped to undergo a successful audit and achieve ISO 27001 certification, assuring clients and partners that your security framework is both robust and compliant with industry standards.

Ai

THE ISO 27001 COMPLIANCE CHECKLIST

1. Establish leadership and define the ISMS scope

- [ ] Engage leadership and relevant stakeholders for commitment.
- [ ] Define which parts of the organization will be included/excluded.
- [ ] Develop a high-level policy outlining ISMS goals and governance.

2. Perform a risk assessment

- [ ] List all internal and external threats to your information security.
- [ ] Assess potential consequences of each risk.
- [ ] Prioritize risks based on likelihood and impact.

3. Design and implement security controls

- [ ] Select appropriate controls from ISO 27001 Annex A based on your risk assessment.
- [ ] Develop clear procedures for each control implementation.
- [ ] Designate owners for each control.

4. Establish a risk treatment plan

- [ ] Decide how to address each risk (mitigate, transfer, accept, or avoid).
- [ ] Create plans with timelines and responsible parties.
- [ ] Track the status of risk treatment actions.

5. Develop an asset management strategy

- [ ] Identify and document all assets within the scope of your ISMS.
- [ ] Categorize assets based on sensitivity and criticality.
- [ ] Ensure that every asset has an assigned owner.

6. Create a statement of applicability (SoA)

- [ ] Record selected controls from Annex A and provide reasoning.
- [ ] Justify any exclusions of controls based on risk profile.
- [ ] Confirm that controls align with identified risks and objectives.

7. Implement employee awareness and training programs

- [ ] Offer training on security policies, procedures, and employee responsibilities.
- [ ] Schedule regular training and security awareness campaigns.
- [ ] Ensure employees know how to report security incidents.

8. Monitor and measure ISMS performance

- [ ] Define measurable indicators to track the effectiveness of your ISMS.
- [ ] Regularly audit internal compliance with ISO 27001.
- [ ] Evaluate control performance against defined KPIs.

9. Prepare for certification audit

- [ ] Perform a gap analysis or mock audit.
- [ ] Organize risk assessments, policies, and audit records.
- [ ] Resolve any issues before the official audit.

10. Address findings and obtain certification

- [ ] Address issues identified during the audit.
- [ ] Provide evidence of corrective actions to the auditor.
- [ ] Acknowledge the achievement and prepare for ongoing compliance.

11. Establish continuous improvement

- [ ] Schedule regular management reviews of the ISMS.
- [ ] Participate in annual surveillance audits.
- [ ] Continuously improve security controls and processes.

12. Leverage automation and tools

- [ ] Use automated tools to track compliance and security incidents.
- [ ] Use systems for tracking performance metrics.
- [ ] Ensure systems generate and maintain audit trails for traceability.

ADDITIONAL TIPS FOR ISO 27001 COMPLIANCE:

- [ ] Ensure all decisions, actions, and risk assessments are thoroughly documented.
- [ ] Secure leadership's support for prioritization and resource allocation.
- [ ] Continuously update your risk assessment as the threat landscape evolves.