ISOPlanner™

ISO 27001 Checklist

1. Obtain Management Commitment

- [ ] Appoint an ISO 27001 team
- [ ] Establish roles and responsibilities
- [ ] Create clarity about the mandate of the project
- [ ] Choose your ISO 27001 compliance software

2. Determine the Scope of Your Project

- [ ] Define which processes are included
- [ ] Assess the current state of your organization with a SWOT analysis
- [ ] Define all relevant stakeholders and expectations everyone has regarding information security
- [ ] Describe the scope of the management system for information security

3. Conduct a Risk Assessment and Select Controls

- [ ] Identify potential information security risks
- [ ] Determine the likelihood that the security risks could occur
- [ ] Evaluate the potential impact of identified risks
- [ ] Rank risks based on your organization's objectives
- [ ] Select appropriate controls for treating all risks

4. Create Policies and Customize Templates

- [ ] Go over the selected controls and determine which policies and procedures will implement them
- [ ] Customize templates with organization-specific policies, processes and language
- [ ] Finalize and publish policies

5. Complete a Statement of Applicability (SoA) Document

- [ ] Review the 93 controls of Annex A of ISO 27001 standard
- [ ] List all Annex A controls and justify the inclusion or exclusion of each control in the ISMS implementation
- [ ] Generate the Statement of Applicability in your ISO 27001 compliance software

ISOPlanner™

ISO 27001 Checklist

6. Embed ISO 27001 Policies and Controls into Your Organization

- [ ] Create a communication plan to inform users
- [ ] Share policies and track employee reviews
- [ ] Perform ongoing control effectiveness monitoring

7. Educate Team Members on ISO 27001

- [ ] Regularly train and educate employees on ISO 27001 and the company's ISMS
- [ ] Provide training on how to respond to the most common risks
- [ ] Educate employees on disciplinary actions that may occur for not being compliant

8. Gather Documentation and Evidence

- [ ] Make sure you have all the required documents and records list for reference during the audit
- [ ] Confirm that you have evidence of monitoring tasks performed in your ISO 27001 compliance software

9. Internal Audit

- [ ] Identify the scope and methodology of an internal audit (clauses 4-10 and applicable Annex A controls)
- [ ] Choose an independent and objective auditor to perform the internal audit
- [ ] Produce and record the internal audit results
- [ ] Remediate any internal audit findings

10. Management Review

- [ ] Gather all information to be discussed in the management review
- [ ] Schedule the management review in your annual plan
- [ ] Perform the management review and save the meeting notes

ISOPlanner™

ISO 27001 Checklist

11. Stage 1 Audit

- [ ] Select an accredited ISO 27001 auditor
- [ ] Conduct a stage 1 audit consisting of an extensive documentation review
- [ ] Obtain feedback regarding readiness to move to a stage 2 audit

12. Stage 2 Audit

- [ ] Conduct a stage 2 audit
- [ ] Implement stage 2 audit advice
- [ ] Address and record specific nonconformities identified by the ISO 27001 auditor

13. Subsequent Audits and Assessments

- [ ] Hold annual or quarterly management reviews
- [ ] Plan for a first and second-year surveillance audit
- [ ] Perform annual risk assessments
- [ ] Plan for a third-year renewal audit
- [ ] Continually ensure the effectiveness of your security objectives
- [ ] Ensure senior management stays informed
- [ ] Ensure prompt implementation of adjustments to address risks or deficiencies

14. Ongoing Improvements

- [ ] Identify and remediate security weaknesses or threats immediately
- [ ] Document and track non-conformities and corrective actions

ISOPlanner™

Effortless ISO 27001 Compliance Management

Structure and control

Structure and control in meeting the ISO 27001 standard

Specific templates

Quick implementation of your ISMS through included sample measures, templates and sample documents

Implement incrementally

A step-by-step, worry-free implementation of the ISO 27001 standard throughout your organization

Implement the ISO 27001 standard quickly and efficiently with ISOPlanner

"SPIE NL IT went through the certification process with a positive result. What contributed in part to this great result was the use of ISOPlanner as an ISMS."

Leon van der Valk - SPIE Nederland B.V.

Watch the demo

Simplify ISO 27001 compliance with rapid deployment in Microsoft 365. Stay compliant.

Watch our demo or contact us!

+31 85 0044933

support@isoplanner.app

www.isoplanner.app

Benefits for your organization

Simple and accessible

Use your Microsoft 365 account and leverage Sharepoint, Outlook, Teams, Dynamics, Azure and Power BI for an integrated and fast compliance experience.

Plan-Do-Check-Act cycle in order

Use Microsoft Power Automate and Power Flow to integrate your compliance controls into your processes.

Trust

Your data never leaves the Microsoft ecosystem.