ISO 27001 Checklist

Read our article on the ISO 27001 checklist

Element	Description
1. Define the scope of application	Determine which information and areas fall within the scope of the ISMS.
2. Statement of Applicability (SoA)	Document the selection of security measures in the Statement of Applicability (SoA), which specific security controls from Annex A are implemented within the defined scope and provide justification for the selection or exclusion of each control.
3. Roles and responsibilities	Clearly define the roles and responsibilities information security in the company. Update your organizational charts and ensure that all employees are aware of the new structure.
4. Information security policy	Develop and document an information security policy that describes the objectives and requirements of the ISMS. This task is performed by the information security officer. They also ensure that all affected employees (with and without PCs) are aware of it. The information security policy must be approved by the organization's management.
5. Identify information values	Identify and classify all information-relevant assets that are important to the organization, including physical, digital and personal information.
6. Risk management process	Implement a process to identify, assess and address information security risks. You should also identify your information assets. This includes IT and non-IT assets. Prepare the inventories and classifications of the assets. This is followed by the risk assessment.
7. Conduct a risk assessment	Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities.
8. Plan and implement risk treatment	Create risk treatment plans, including the selection of suitable security measures. Define the responsibilities for the planned measures and monitor their implementation.
9. Create ISMS documentation	Create and maintain required documentation, including supporting policies, procedures and work instructions.

10. Employee training and awareness	Train and raise awareness among employees regarding information security policies and procedures regularly.
11. Manage security incidents	Implement procedures for detecting, reporting and handling security incidents.
12. Emergency management	Develop and test contingency plans to ensure business continuity if a security incident occurs.
13. Monitoring and measurement	Regularly monitor and measure the performance of the ISMS and compliance with the security guidelines using defined KPIs.
14. Internal Audits	Conduct regular and independent internal audits to check the effectiveness of the ISMS and identify vulnerabilities.
15. Corrective measures	Implement corrective measures to address non-conformities and improve the ISMS.
16. Management review	Conduct regular management reviews to ensure the suitability, adequacy and effectiveness of the ISMS.
17 External audit and certification	Prepare for the external audit and work with the certification company to achieve ISO 27001 certification.
18 Continuous improvements	Implement processes to continuously improve the ISMS based on the results of monitoring, audits and assessments.