Melbourne, Australia- 80014
www.informationsecurityconsultants.com.au | 1300887463

ISO 27001:2022 Checklist

Purpose

By systematically going through the checklist, organisations can identify gaps and areas of non-conformity within their ISMS. This enables them to prioritise corrective actions and improvements to enhance their security posture.

ISO 27001: 2022 Domain	Checklist
Management Support (5.1)	• Gain commitment from top management for implementing ISO 27001. • Appoint a management representative to oversee the implementation.
Scope Definition (4.3)	• Define the scope of the ISMS, including boundaries, assets, and processes to be covered.
Issues and Interested parties(Clause 4.1 and 4.2)	• Determine internal and external issues relevant to ISMS • Determine interested parties that can affect your ISMS and their requirements.
Risk Assessment (Clause 8)	• Identify and assess information security risks. • Determine the likelihood and impact of each risk. • Prioritize risks for treatment based on their significance.
Risk Treatment (Clause 8)	• Develop and implement risk treatment plans to address identified risks. • Select appropriate controls to mitigate or manage risks. • Document procedures and responsibilities for implementing controls.

Information Security Policy (Clause 5.2)	• Develop an information security policy that aligns with the organization's objectives and legal/regulatory requirements. • Obtain approval from top management and communicate it to all relevant stakeholders.
Documentation (Clause 7 Support)	• Establish and maintain documentation of the ISMS, including policies, procedures, and records. • Ensure documentation is accessible, up-to-date, and effectively communicated.
Resource Allocation (Clause 7 Support)	• Allocate necessary resources (human, financial, and technological) for implementing and maintaining the ISMS.
Competence, Awareness, and Training Clause 7 Support)	• Identify competency requirements for personnel involved in the ISMS. • Provide appropriate training and awareness programs on information security roles, responsibilities, and procedures.
Monitoring and Measurement (Clause 9 Performance evaluation)	• Establish processes to monitor, measure, and analyze the performance of the ISMS. • Define key performance indicators (KPIs) to track the effectiveness of security controls and processes.
Internal Audits (Clause 9)	• Conduct regular internal audits to assess compliance with ISO 27001 requirements and the effectiveness of the ISMS. • Ensure auditors are independent and competent to perform audits.

Management Review (Clause 9)	• Conduct periodic management reviews to evaluate the performance of the ISMS. • Review audit findings, corrective actions, and improvement opportunities. • Make decisions regarding ISMS improvements and resource allocation.
Continuous Improvement (Clause 10)	• Implement corrective actions to address non-conformities and improve the effectiveness of the ISMS. • Continuously monitor and review the ISMS to adapt to changes in the organization, technology, and security threats.

Adhering to this checklist will help ensure a systematic and structured approach to implementing ISO 27001 within your organisation, leading to improved information security practices and risk management capabilities.