

# ISO 27001 Checklist

## 1. Appoint an ISO 27001 team

- Establish roles and responsibilities

## 2. Build your ISMS

- Define the scope of your ISMS
- Inform leadership regarding the ISMS scope

## 3. Create and publish ISMS policies, documents, and records

- Build a framework for establishing, implementing, maintaining, and continually
- Customize policy templates with organization-specific policies, processes, and language
- Finalize and publish policies

## 4. Conduct a risk assessment

- Establish a risk management framework
- Identify potential risks
- Determine the likelihood that these risks could occur
- Evaluate the potential impact of identified risks
- Rank risks based on the overall risk to your organization's objectives
- Create a response plan for each risk

## 5. Complete a Statement of Applicability (SoA) document

- Review 114 controls of Annex A of ISO 27001 standard
- Select controls to address identified risks

- Complete the Statement of Applicability, listing all Annex A controls and justifying inclusion or exclusion of each control in the ISMS implementation

## 6. Implement ISMS policies and controls

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

## 7. Train team members on ISO 27001

- Hold regular trainings to educate employees on ISO 27001 and the company's ISMS
- Provide training on how to respond to the most common risks your organization faces
- Educate employees on disciplinary actions that may take place if they are out of compliance with data security requirements

## 8. Gather documentation and evidence

- Prepare ISO 27001 Required Documents and Records list for reference during audit

## 9. Undergo internal audit

- Identify scope and methodology of 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. Undergo a stage 1 audit

- Select an accredited ISO 27001 auditor

- Conduct Stage 1 audit consisting of an extensive documentation review
- Obtain feedback regarding readiness to move to Stage 2 audit

### 11. Implement Stage 1 audit advice

- Ensure that all requirements of the ISO 27001 standard are being addressed
- Ensure organization is following processes that it has specified and documented
- Ensure organization is upholding contractual requirements with third parties
- Address and record specific nonconformities identified by the ISO 27001 auditor

### 12. Undergo a Stage 2 audit

- Conduct stage 2 audit

### 13. Implement Stage 2 audit advice

- Address and record specific nonconformities identified by the ISO 27001 auditor

### 14. Commit to subsequent audits and assessments

- Hold management reviews annually or quarterly
- Prepare for first- and second-year surveillance audits
- Perform annual risk assessments
- Prepare for third-year renewal audit
- Ensure the ISMS and its objectives continue to remain appropriate and effective
- Ensure that senior management remains informed
- Ensure adjustments to address risks or deficiencies can be promptly implemented

### 15. Perform ongoing improvements

- Ensure weaknesses/threats to the ISMS are identified and remediated
- Document and track non-conformities and corrective actions to closure