

GUIDE

ISO 27001 Certification Readiness Guide

A practical guide for first-time organisations that breaks the path to ISO 27001 certification into simple steps.



GUIDE

ABOUT 7 MIN READ

ISO 27001

IN THIS GUIDE

1. What is ISO 27001 and what does it give you?
2. Roadmap: certification in six steps
3. Getting the scope right
4. Risk assessment and the Statement of Applicability (SoA)
5. Pre-audit checklist
6. Common mistakes

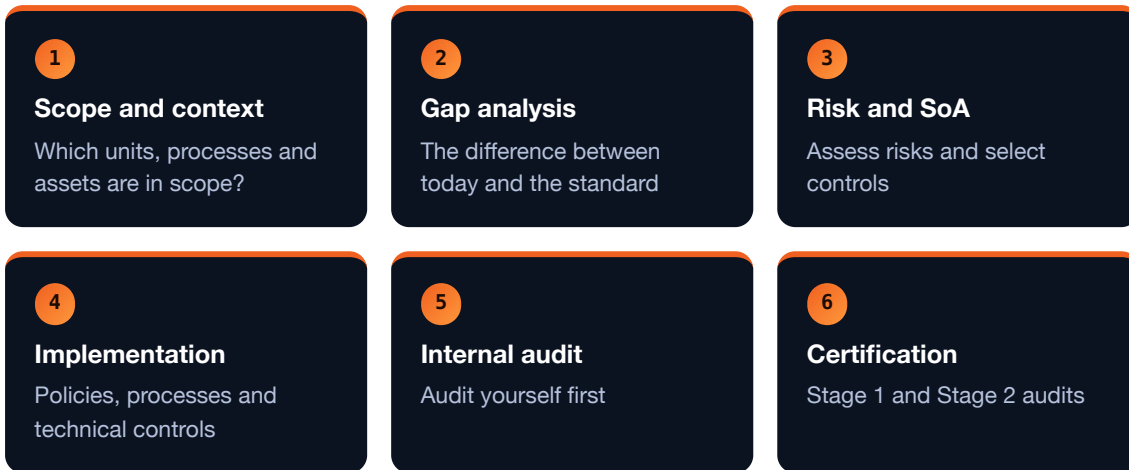
01 What is ISO 27001 and what does it give you?

ISO 27001 is the international standard that defines the requirements for an Information Security Management System (ISMS). Its aim is to turn information security from something left to individuals and tools into a risk-based management system that is continually improved. Certification is granted after audits by an independent certification body and is typically valid for three years, with annual surveillance audits in between.

Why it matters: Customers and tenders increasingly ask for ISO 27001. The real value, however, is managing risks knowingly and being able to prove it.

02 Roadmap: certification in six steps

Duration differs for every organisation, but the order is almost always the same:



03 Getting the scope right

Scope is the foundation of every later step. Too broad and the project drags; too narrow and the certificate loses value.

- Which business units, locations and processes are in scope?
- Which information assets and systems do these processes rely on?
- What dependencies exist on suppliers and cloud services?
- If an area is excluded, is the reason documented?

Tip: You can start with a narrow scope and widen it in later years.

04 Risk assessment and the Statement of Applicability (SoA)

The standard does not ask you to apply a ready-made checklist but to choose controls based on your risks.

- Inventory your information assets and assign owners.
- Identify threats and vulnerabilities and rate likelihood and impact.
- Decide a treatment for each risk: reduce, transfer, accept or avoid.
- Show in the SoA which of the 93 Annex A controls (ISO 27001:2022) are applied and which are excluded, with reasons.

05 Pre-audit checklist

- | | |
|--|---|
| ☐ Scope statement approved | ☐ Information security policy published and communicated |
| ☐ Risk assessment and treatment plan up to date | ☐ SoA ready and current |

☐ Internal audit done and findings closed	☐ Management review held and recorded
☐ Awareness training and incident records available	☐ Corrective actions documented

06 Common mistakes

- Piling up documents and skipping real implementation
- Not securing management support and resources up front
- Filling in the risk assessment as a formality
- Running the internal audit late and superficially
- Choosing an over-broad scope that stretches the project

Let's start your ISO 27001 journey together We will assess your current state and build a roadmap that fits.

// CONTACT

Get in touch

Share your needs and current situation and we will define the right scope and roadmap together. Fill in our information form or contact us directly.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul, Türkiye

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Scan the QR code for the service page and information form