ISO 27001 Readiness Checklist

a

PRIVALEX

checklist

ISO 27001 is the international gold standard for information security. It defines how to build an Information Security Management System (ISMS) that protects sensitive data, reduces risk, and demonstrates trust to clients, partners, and regulators.

For many CEOs and compliance leaders, ISO 27001 is the entry point to structured cybersecurity, but it can feel complex at first glance.

This guide gives you:

- A simple readiness checklist.
- A clear view of the benefits.
- An honest look at the challenges and risks.

BENEFITS OF ISO 27001 CERTIFICATION

TRUST, REPUTATION AND MARKET CREDIBILITY

Organisations certified under ISO 27001 demonstrate that they manage information security in a systematic, mature and verifiable way. This strengthens trust among clients, partners and investors, enhances corporate reputation, and positions the company as a reliable and professional provider.

ACCESS TO NEW BUSINESS OPPORTUNITIES

An increasing number of companies and public authorities require ISO 27001 as a prerequisite in procurement processes, tenders and agreements with technology providers. Holding the certification facilitates access to new markets, accelerates sales processes and removes barriers in B2B and enterprise sales.

RISK REDUCTION AND GREATER OPERATIONAL CONTROL

ISO 27001 helps organisations continuously identify, manage and reduce information security risks. This lowers the likelihood of incidents, data breaches and operational disruptions, reducing financial, legal and reputational impacts on the organisation.

SCORING YOUR READINESS

8–10 Yes / Completed: Strong readiness.
You're on the right track, but you'll need to review specific details to fully meet the requirements.

4–7 Yes / Completed: Moderate risk.
The gaps may expose you to fines, delays or incidents. Prioritise resolving them.

0–3 Yes / Completed: High risk.
Immediate action is needed to prepare for compliance and reduce exposure.

**for each question, choose one option::*

1 Scope & Context

Have you defined the scope of your ISMS (which systems, processes, locations) and documented it?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Do you understand the technological, legal, and contractual requirements that drive security in your context?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

2 Leadership & Responsibility

Do you have top management buy-in for ISO 27001?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Have you established a Security Committee and appointed the ISMS owner?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

3 Risk Assessment & Treatment

Do you have a formal process for identifying, assessing, and mitigating information security risks?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Have you defined risk acceptance criteria (what's tolerable vs. not tolerable)?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

4 Security Controls (Annex A)

Do you have baseline measures in place (e.g., access control, encryption, backups)?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Are your technical, physical, and organizational controls aligned with the risks you have identified and assessed?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

5 Policies & Procedures

Have you created key information security policies (e.g., acceptable use, incident response, supplier management)?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Are policies communicated and followed across the business?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

**En cada pregunta, marca una opción:*

6 Training & Awareness

Do your employees receive regular security and privacy training?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Is security culture embedded in daily operations?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

7 Incident Management

Do you have a documented incident response plan?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Can you log, escalate, and report incidents in a structured way?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

8 Supplier & Third-Party Risk

Do you evaluate the security posture of critical suppliers?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Are contracts aligned with security and compliance requirements?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

9 Internal Audits & Reviews

Do you conduct internal audits of security practices?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Does management perform a regular review of the ISMS?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

10 Continuous Improvement

Do you have a process for corrective actions and continuous improvement?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

Are you monitoring and adapting to new threats and requirements?

☐ *Yes / Completed* ☐ *In progress* ☐ *No / Not yet started*

MAIN RISKS OF NOT BEING ISO 27001 READY

Increased exposure to security incidents
Lack of structured controls increases the likelihood of data breaches, ransomware attacks and operational disruptions.

Loss of trust and commercial opportunities
Clients, partners and investors increasingly expect demonstrable information security maturity. Without it, deals stall or fail.

Regulatory and contractual exposure
Security incidents can trigger regulatory scrutiny, contractual penalties and liability claims.

Inefficient and reactive security management
Without an ISMS, security efforts remain fragmented, reactive and difficult to scale as the business grows.

KEY CHALLENGES ORGANISATIONS FACE WITH ISO 27001

1. Defining a realistic and well-scoped ISMS
Overly broad or unclear scopes create unnecessary complexity and slow down certification.

2. Translating requirements into real, workable controls
ISO 27001 is not about documentation alone, controls must be implemented, used and maintained in daily operations.

3. Engaging leadership and the wider organisation
Without top management support and employee awareness, the ISMS becomes a paper exercise rather than a living system.

4. Maintaining momentum over time
Risk assessments, audits and improvements must be continuous, not one-off efforts tied only to certification.

NEXT STEPS

At PrivaLex Partners, we help organisations turn ISO 27001 requirements into practical, business-ready controls.

From scoping and risk management to implementation and training, we make certification achievable and sustainable.

CONTACT US **IF YOU ARE INTERESTED IN ACHIEVING ISO 27001 COMPLIANCE WITH**

PRIVALEX