Agency

THE STARTUP COMPLIANCE SERIES · CHECKLIST

ISO 27001

The startup

ISO 27001 Readiness Checklist

Everything your ISMS needs in place before certification — in one place you can actually use.

A practical companion checklist for founders & engineering leaders

© Agency Cyber Inc. 2026

June 22, 2026 • getagency.com

ISO 27001 · READINESS CHECKLIST

How to use this checklist

This is the short, high-level version of what a certification body looks for — organized the way you'll actually build it. It won't replace a formal readiness assessment, but in about ten minutes it'll tell you roughly how ready your ISMS is and where the gaps are.

Score yourself honestly: ■ done · ◪ partial · ☐ not started. If you finish with a lot of ◪ and ☐, that's normal for a first-timer — it just shows how much ISMS work is ahead and which path makes sense for getting it done.

> **A quick reminder before you start:** ISO 27001 certifies a *living management system*, not a checklist. This list tells you *what* needs to be true; it doesn't run the risk assessment, conduct the internal audit, or make the judgment calls for you. Keep that gap in mind as you tally your score.

---

1. ISMS scope & foundations

Get these decisions right first — they shape the whole certification.

- ◇ Defined the **ISMS scope** (which products, teams, locations, and data are covered)
- ◇ Identified **internal and external issues** and **interested parties** (the "context" the standard asks for)
- ◇ Confirmed your **target certificate** and rough timeline (Stage 1 → Stage 2)
- ◇ Named a clear **ISMS owner** with the time and authority to run it
- ◇ Understood the **three-year cycle** (certification + annual surveillance + recertification)

2. Leadership & governance

ISO 27001 explicitly requires leadership involvement — this isn't optional.

- ◇ **Information Security Policy** approved by leadership
- ◇ Documented **security objectives** that ladder up to the business
- ◇ **Roles and responsibilities** for security assigned
- ◇ Evidence of **leadership commitment** (resourcing, oversight, decisions)

3. Risk assessment & treatment

The engine of the whole standard.

- Documented **risk assessment methodology**
- Completed a **risk assessment** with identified risks, owners, and ratings
- Maintained a **risk register** that stays current
- **Risk treatment plan** deciding how each risk is handled
- **Statement of Applicability (SoA)** listing each Annex A control with applied / not-applied and justification

4. Annex A — Organizational controls

Policies, processes, and governance (the largest Annex A theme).

- Core security **policies** written and acknowledged by staff
- **Access control** policy and least-privilege approach
- **Supplier / third-party security** management
- **Incident management** process defined
- **Business continuity** considerations documented
- Awareness of **legal, regulatory, and contractual** requirements

5. Annex A — People controls

The human side of the ISMS.

- **Screening / background checks** where appropriate
- **Security awareness training** at onboarding and ongoing
- **Confidentiality / NDA** terms in employment agreements
- Defined **onboarding and offboarding** (including access removal)
- A process for **reporting security events**

6. Annex A — Physical controls

Even cloud-first startups need to address these.

- **Physical access** to offices / sensitive areas controlled
- **Clear desk / clear screen** expectations
- **Secure handling and disposal** of equipment and media

- Reliance on **cloud providers' physical security** documented (e.g., their certifications)

7. Annex A — Technological controls

The technical backbone.

- **MFA and strong authentication** enforced
- **Encryption** in transit and at rest
- **Logging and monitoring** in place
- **Vulnerability management** and patching cadence
- **Secure development / change management** practices
- **Backups** configured and tested
- **Endpoint protection** and network controls
- **Data protection / segregation** in environments

8. Operate the ISMS

ISO wants proof the system actually runs — not just that it exists.

- ISMS **operating procedures** documented and followed
- **Internal audit** of the ISMS completed at least once
- **Management review** held and recorded
- **Corrective actions / continual improvement** tracked
- **Metrics / monitoring** of how well controls are working

9. Certification prep

Where a running ISMS turns into a certificate.

- **Mandatory documentation** complete (scope, policy, risk method, SoA, risk treatment plan, objectives, internal audit and management review records)
- Evidence is **collected continuously**, not reconstructed at the deadline
- Engaged an **accredited certification body** and aligned on timeline
- Ready for **Stage 1** (documentation review) and **Stage 2** (implementation review)
- A clear **owner** for auditor requests and closing nonconformities

Now the real question: who's going to run all this?

If you scored mostly ☐ and ◪, don't panic — that's the normal starting point. The harder question isn't *what's on the list*; it's *who runs the system*. ISO 27001 is process-heavy, so this matters even more than with SOC 2. Three common answers:

Do it yourself with spreadsheets. Workable for very early, security-savvy teams with time to spare — but a management system in spreadsheets drifts, and the risk register, internal audit, and management review are easy to let slip.

Buy a GRC platform like Vanta or Drata and run it yourself. A big step up: these tools support ISO 27001, map controls, help manage the risk assessment and SoA, and automate evidence collection. Just remember a platform organizes the ISMS — it doesn't run your risk workshop, conduct your internal audit, or make SoA judgment calls. It assumes a capable system owner in-house.

Have it operated for you. A dedicated team runs the ISMS end to end — usually on top of a platform like Vanta or Drata — including risk assessment, internal audit coordination, remediation, and certification-body coordination, so your engineers stay on the roadmap and you certify right the first time.

(For a deeper breakdown of these three paths and how to choose, see our companion piece, The Startup's Guide to Buying ISO 27001.)

Where Agency fits

This checklist comes from **Agency** — a security and compliance team you don't have to hire. U.S.-based forward-deployed engineers, supercharged by our own AI, run your ISO 27001 end to end on top of the tools you already trust like **Vanta** and **Drata**: virtual CISO, risk assessments, control implementation, internal audit coordination, evidence collection, continuous monitoring, vendor risk, and certification-body coordination, all included without adding headcount. Agency has served more than 1,000 companies — across ISO 27001, SOC 2, and beyond — and is backed by Y Combinator.

Want us to turn this checklist into a certification-ready ISMS?
Get a free readiness review — we'll tell you where your ISMS stands and the fastest path to certified.

Assemble your GRC team ›

This checklist is for general educational purposes and isn't legal, audit, or compliance advice. Your specific requirements depend on your business, systems, risk profile, and customer commitments.