Agency

THE STARTUP COMPLIANCE SERIES · GUIDE

ISO 27001

The startup's guide to

# Buying ISO 27001

How to earn one of the world's most recognized information security certifications without derailing your roadmap.

A practical buyer's guide for founders & engineering leaders

© Agency Cyber Inc. 2026

June 22, 2026 • getagency.com

ISO 27001 · STARTUP GUIDE

## Why you're reading this

For most startups, ISO 27001 shows up the moment you start selling beyond your backyard.

An enterprise prospect in Europe asks whether you're "ISO certified." A global customer's procurement team won't even start a security review without it. A partner makes it a contractual requirement. SOC 2 may have unblocked your U.S. deals — but internationally, ISO 27001 is often the standard buyers recognize and trust by name.

The good news: ISO 27001 is a globally established, well-documented path, and thousands of companies certify every year. The bad news: it's heavier on process than SOC 2, wrapped in its own vocabulary (ISMS, Annex A, SoA, surveillance audits), and easy to over-build if you don't know where the real requirements stop.

This guide is written for the first-timer. No prior compliance background assumed. By the end you'll understand what ISO 27001 actually is, how it differs from SOC 2, the handful of decisions that matter, the three ways startups typically get certified, and how to choose the path that fits your stage. We've kept it high level and practical — a buyer's guide to the lay of the land. It's written by the team at Agency; we've worked to compare the options fairly, and we're upfront that we also offer the operated approach covered later, so you can weigh our perspective accordingly.

---

## ISO 27001 in plain English

ISO/IEC 27001 is the international standard for an **Information Security Management System** — an ISMS. Rather than auditing a fixed list of controls, it certifies that you've built a *system for managing security*: identifying risks, deciding what to do about them, putting controls in place, and continually improving over time.

A few things worth understanding up front:

**It's a certificate, not just a report.** This is the big difference from SOC 2. When you pass, an independent, accredited certification body issues a formal certificate (valid for three years, subject to ongoing checks). You can state that you're "ISO 27001 certified" — a claim international buyers recognize instantly.

**It's a management system, not a one-time checklist.** The heart of ISO 27001 is the ISMS: a living set of processes for governing security. Auditors care as much about whether the *system* runs — risk reviews, internal audits, management reviews — as about any individual control.

**It's risk-based.** You're not told exactly which controls to implement. You assess *your* risks, then decide which controls address them and justify your choices. This flexibility is the standard's strength — and where first-timers most often get lost.

**It has two halves: the clauses and Annex A.**

- **The management clauses (4–10)** are mandatory. They cover the context of your organization, leadership commitment, planning, support, operation, performance evaluation, and improvement. This is the ISMS itself.
- **Annex A** is a catalogue of **93 security controls** grouped into four themes — **Organizational, People, Physical, and Technological** (this is the structure introduced in the 2022 version of the standard). You select the ones relevant to your risks.

**The Statement of Applicability (SoA)** is the document that ties it together: it lists every Annex A control and records whether you've applied it, and why or why not. It's the centerpiece auditors return to again and again.

**It's a multi-year commitment.** Certification runs on a three-year cycle (more on that below). The first certification is the heavy lift; staying certified becomes a rhythm.

---

## The thing that trips everyone up: it's a system, audited in stages

Two ideas confuse first-timers more than anything else.

**First — you're certifying a system, not a snapshot.** Plenty of teams try to "do ISO" like a checklist sprint, then discover the auditor wants evidence that the ISMS has actually been *operating*: that risk assessments happened, that an internal audit was run, that leadership reviewed the program. You can't manufacture a management system the week before. The processes need to have been running.

**Second — certification happens in stages, then repeats.** The journey isn't a single exam:

- **Stage 1 audit** — the certification body reviews your ISMS documentation to confirm you're ready. Think of it as a readiness gate.
- **Stage 2 audit** — they examine whether your ISMS is actually implemented and effective in practice. Pass this and you're certified.
- **Surveillance audits** — lighter check-ins (typically annual) to confirm the ISMS keeps running.
- **Recertification** — around the three-year mark, a fuller audit renews the certificate for another cycle.

The practical takeaway: the biggest predictor of a smooth certification isn't the certification body you pick — it's how genuinely your security management system runs day to day. Evidence the ISMS produces naturally beats evidence you assemble under deadline.

---

## What the journey actually looks like

Strip away the jargon and the path has four phases:

**1. Build the ISMS (readiness).** Define your scope, secure leadership buy-in, run a risk assessment, decide how you'll treat each risk, select your Annex A controls, write the required policies and procedures, and produce your Statement of Applicability. This is where most of the effort lives.

**2. Operate it.** Let the ISMS run for a period — risks get reviewed, controls operate, and you complete at least one **internal audit** and a **management review** before the certification audit. (Auditors expect to see these.)

**3. Get audited (Stage 1, then Stage 2).** The certification body reviews your documentation, then tests implementation and effectiveness. You close any nonconformities they raise.

**4. Certify — then maintain.** You receive your certificate, valid for three years, and share it with prospects. Surveillance audits keep it active, and recertification renews it. ISO 27001 rewards companies that treat security as an ongoing discipline.

---

## ISO 27001 vs. SOC 2 — a quick orientation

If you've already done SOC 2 (or are weighing both), here's the short version:

- **SOC 2** is a U.S.-rooted **attestation report** describing your controls against the Trust Services Criteria. Buyers' security teams read the report.
- **ISO 27001** is an **international certification** of a management system. Buyers recognize the certificate by name, often without reading anything further.
- The **underlying controls overlap heavily** — encryption, access control, monitoring, vendor risk, incident response all appear in both. If you've done one, you're well down the road to the other.
- ISO leans more on **governance and continual improvement** (the ISMS); SOC 2 leans more on **evidencing controls over an observation window**.

Many startups end up pursuing both — SOC 2 for North American buyers, ISO 27001 for international ones. The smart move is to build one security operation that serves multiple frameworks, rather than running each as a separate fire drill.

---

## The three ways startups get ISO 27001 done

Once you understand what ISO 27001 requires, the real question is *how you'll actually do the work*. There are three common paths.

### Path 1 — DIY without a GRC platform

You build and run the ISMS with spreadsheets, shared drives, and document templates. You write the policies, maintain the risk register by hand, draft the SoA in a spreadsheet, and gather evidence manually.

**Who it can fit:** Very early teams with a strong technical or security-minded lead who has built an ISMS before, a simple scope, and more time than money.

**The honest tradeoffs:** ISO 27001 is process-heavy, and that weight lands hardest on the DIY path. A management system maintained in spreadsheets tends to drift; the risk register goes stale; the internal audit and management review get skipped because no one owns them. When the certification body asks for evidence the ISMS has been running, you're reconstructing it instead of presenting it. For most startups, "free" quietly becomes the most expensive option in founder and engineer hours.

### Path 2 — Buy a GRC platform (e.g., Vanta or Drata) and run it yourself

GRC automation platforms like **Vanta** and **Drata** support ISO 27001: they connect to your stack, map your controls, help manage the risk assessment and SoA, automate evidence collection, and track readiness against the standard.

**Who it can fit:** Teams that want structure and automation and have someone in-house with the time and judgment to operate the platform, run the ISMS, and drive the work to certification.

**The honest tradeoffs:** This is a major step up from spreadsheets, and these platforms are very good at what they do. But it's important to understand what they *are*: they automate **evidence collection, control mapping, and monitoring**. They are not a person. The platform won't run your risk workshop, make the judgment calls in your SoA, conduct your internal audit, write the remediation for a failing control, or sit across from the certification body on your behalf. ISO 27001 in particular demands human-driven activities — leadership engagement, risk treatment decisions, internal audits, management reviews — that a tool can organize but not perform. Buy a platform expecting a tool and you'll get the value; expect it to run your ISMS and you'll be disappointed.

### Path 3 — Have it operated for you

Instead of just buying software, you bring in a team that *runs* the ISMS end to end — typically on top of a platform like Vanta or Drata, not instead of it. They handle scoping, lead the risk assessment, build the SoA, write and tailor policies, implement and remediate controls, coordinate or conduct internal audits with appropriate independence, facilitate the management review with your leadership, collect and validate evidence, and coordinate with the certification body through Stage 1 and Stage 2. You get the dashboard *and* the people who operate it.

**Who it can fit:** Startups who'd rather their engineers ship product than become part-time ISMS managers — and who want certification done right the first time, with security maturity that holds up across the full three-year cycle.

**The honest tradeoffs:** You're adding a partner rather than doing it all internally, so it works best when you value speed, certainty, and keeping your team focused on the roadmap. The upside: the governance-heavy work that usually falls on your most senior people — risk decisions, internal audits, remediation, audit wrangling — is handled by people who do it every day.

---

## The work a platform doesn't do

This surprises most first-timers with ISO 27001 even more than with SOC 2, because the standard is so process-driven. Whether you go DIY or buy a platform, *someone* still has to:

- Define the right **scope** so you're not certifying more than your buyers need.
- Run a real **risk assessment** and make **risk treatment** decisions — judgment calls a tool can't make for you.
- Build and justify the **Statement of Applicability**, control by control.
- Write and tailor **policies and procedures** to how your company actually operates.
- Implement the real technical and organizational controls — and **remediate** the ones that fall short.
- Conduct **internal audits** with appropriate independence, and facilitate the **management review** with leadership, as the standard requires.
- Drive **leadership engagement** and **continual improvement**, not just at audit time.
- Manage **Stage 1 and Stage 2**, close nonconformities, and keep the ISMS running through surveillance and recertification.

Automation removes the busywork of *gathering* evidence and *organizing* the ISMS. It doesn't remove the **judgment and governance** of actually running an information security management system. The three paths above are really three answers to one question: *who is going to run this system?*

---

## How to choose: a quick framework

Run your situation through these five questions.

1. **How urgent is the deal — and is it international?** If a global contract is gated on ISO 27001, you need a path that gets you to a successful Stage 2 dependably. Pure DIY is the slowest and least predictable.

2. **How much engineering and leadership time can you actually spare?** ISO 27001 pulls in founders and senior staff (leadership commitment is part of the standard). Be honest about that cost in dollars and roadmap.
3. **Do you have in-house ISMS expertise?** Has anyone run a management system, a risk assessment, or an internal audit before? A platform assumes a competent operator; ISO assumes a competent *system owner*.
4. **Is this one certificate or part of a broader program?** If SOC 2, HIPAA, or other frameworks are also in play, build one security operation that serves all of them rather than standing up ISO in isolation.
5. **What's the cost of getting it wrong?** A failed or delayed Stage 2, unresolved major nonconformities that hold up certification, or a lapsed surveillance audit can undermine trust with the exact international buyers you're chasing.

A simple rule of thumb: **the heavier the governance burden and the higher the stakes, the further down the path from DIY → platform → operated you should look.** ISO 27001's process weight pushes more teams toward help than SOC 2 does.

---

## Common first-timer mistakes to avoid

- **Over-scoping the ISMS.** Pulling every system and team into scope multiplies the work for no commercial benefit. Scope to what your buyers actually need certified.
- **Treating it as a checklist, not a system.** ISO certifies a *living* ISMS. Skipping the internal audit, management review, or risk reviews is the fastest way to fail Stage 2.
- **Starting the audit before the ISMS has run.** Auditors want evidence the system has been operating — you can't backfill a management review.
- **Treating a tool as a team.** A platform organizes the ISMS; it doesn't make risk decisions or conduct your internal audit.
- **Neglecting leadership involvement.** "Leadership commitment" is an actual requirement, not a formality. Absentee leadership shows up as a finding.
- **Letting surveillance lapse.** Certification is a three-year cycle. Miss the rhythm and you risk the certificate.

---

## What "good" looks like

A healthy ISO 27001 program, regardless of who runs it, tends to share a few traits:

- **Scope is right-sized** to what your customers actually require.

- **Risk drives the controls** — your SoA reflects real decisions, not a generic copy-paste.
- The **ISMS genuinely runs**: risk reviews, internal audits, and management reviews happen on schedule.
- **Evidence is generated continuously**, not reconstructed before Stage 2.
- Someone clearly **owns the system** and has the authority to drive it.
- The audit is **a confirmation, not a surprise** — and surveillance years get easier, not harder.

If your plan doesn't get you to most of these, it's worth rethinking the path before you start.

---

## A note on doing this without distracting your team

Most startups don't fail ISO 27001 because the standard is impossible. They struggle because building and running an ISMS quietly pulls their best people off the roadmap for months — assessing risk, writing policies, implementing controls, running internal audits, and coordinating with a certification body — none of which is why they joined.

That's the case for the operated approach, and it's worth being upfront that this guide comes from **Agency**. We're a security and compliance team you don't have to hire — U.S.-based forward-deployed engineers, supercharged by our own AI, who run your program 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 — included, without adding headcount. Agency has served more than 1,000 companies — across SOC 2, ISO 27001, and beyond — and is backed by Y Combinator.

Whichever path you choose, we hope this guide makes the decision clearer. If you'd like a second opinion on your specific situation — scope, timeline, and the fastest route to successful certification with no avoidable nonconformities — we're happy to talk.

**Want to see what an operated ISO 27001 would look like for your startup?**
Talk to our team for a no-pressure walkthrough of your scope and timeline.

**Assemble your GRC team ›**

---

*This guide is for general educational purposes and isn't legal, audit, or compliance advice. ISO 27001 requirements depend on your specific business, systems, risk profile, and customer commitments.*