SOC 2 vs ISO 27001: which does a European startup actually need

Most guides answer this from a North American desk, where SOC 2 is the default. If you sell from Europe, the honest answer is usually the other one. Here is how to decide, what each costs, and why the choice is the buyer's, not yours.

Published 2026-07-01 · A Mue guide

A prospect asks for your "security certification" and you go looking. Every second guide tells you to get SOC 2. Most of those guides are written from a North American desk, where SOC 2 is the default ask. If you are selling from Europe, the honest answer is usually the other one, and the two are not interchangeable deliverables.

The short answer: the buyer decides, not you

This is not a matter of taste. Which one you need is set by the customer in front of you. North American enterprise buyers overwhelmingly ask for SOC 2. European and international buyers, and most public-sector and regulated procurement, recognise ISO 27001. If a specific deal has named a standard, that is the one to get. If nobody has specified and your pipeline is mostly European, ISO 27001 is the safer default because it is recognised in more places.

What each one actually is

- SOC 2 is an attestation. A licensed CPA firm examines your controls against the Trust Services Criteria and writes a report. A Type I attests the controls are designed correctly at a point in time; a Type II attests they operated effectively across a window, commonly three to twelve months. You refresh the report every year.
- ISO 27001:2022 is a certification. You build a working information security management system (the ISMS), a certification body audits it in two stages (Stage 1 reviews your documentation, Stage 2 tests whether the controls are actually followed), and you get a certificate valid for three years.

That structural difference, a yearly attestation report versus a three-year certificate, is what makes the two feel different to live with, and it is where the cost shapes diverge.

What each costs in year one

The auditor invoice is only one of four lines, and usually not the biggest. Reusing the planning bands the estimator runs on:

- SOC 2 Type II auditor fee: roughly 12,000 to 30,000 dollars.
- ISO 27001:2022 Stage 1 plus Stage 2 audit: roughly 14,000 to 38,000 dollars.
- Compliance-automation tooling: a band from about 7,000 to 30,000 dollars a year

depending on headcount and how many frameworks you run.

- Independent penetration test: about 4,000 to 12,000 dollars, expected by auditors and enterprise buyers for either standard.

On top of those sits your own team’s time, writing policies, wiring up logging and assembling evidence, which is typically the single largest line for either framework. So the two land in a broadly similar first-year range, with ISO 27001 often slightly higher because the two-stage audit plus the required management system (with its own mandatory internal audit and management review) add work.

Where the renewal economics diverge

They cost about the same to start and then behave differently. SOC 2 is a report you commission again every year, so year two looks a lot like year one. ISO 27001 front-loads the effort: after the initial certification, years two and three are lighter surveillance audits that sample a subset of controls rather than re-examining the whole ISMS, and a fuller recertification audit comes at the end of the three-year cycle. If you expect to hold a standard for years, ISO 27001’s renewal path is the cheaper one; if you are not sure you will keep it, SOC 2’s pay-as-you-go yearly cadence carries less commitment.

If you might need both, the overlap pays

Plenty of teams selling on both sides of the Atlantic end up needing both. The good news is that the two frameworks share most of their underlying controls, so the evidence you gather for one does most of the work for the other. The estimator reflects this: a combined SOC 2 Type II plus ISO 27001 auditor engagement lands around 22,000 to 55,000 dollars, which sits below the roughly 26,000 to 68,000 you would pay for two separate audits, and one automation platform covers both rather than doubling the tooling bill.

The European trap: ISO 27001 is not GDPR

This one catches European founders often. ISO 27001 is an information security certification; the GDPR is a data-protection law, and they are not the same thing. Holding ISO 27001 helps you demonstrate the "security of processing" that Article 32 of the GDPR requires, and it is strong evidence of good practice, but it does not make you GDPR compliant on its own, and there is no official GDPR certificate you can buy. You still need a lawful basis for processing, data-subject request handling, records of processing and the rest. Treat ISO 27001 as the security half of the story, not the whole of your data-protection obligations.

Pick the standard your buyers actually ask for, budget for all four cost lines rather than just the auditor, and if the answer is "both", lean on the overlap instead of running two projects in parallel.

Frequently asked questions

SOC 2 or ISO 27001: which does a European startup need?

Let the buyer in front of you decide. North American enterprise customers usually ask for SOC 2, an AICPA attestation report. European and international buyers, and most public-sector procurement, recognise ISO 27001, a globally accepted certification. If a specific prospect has named one, get that one. If nobody has specified and your pipeline is mostly European, ISO 27001 is the safer default because it travels further.

Is ISO 27001 more expensive than SOC 2?
In year one they land in a similar range, with ISO 27001 often slightly higher. A SOC 2 Type II auditor fee runs roughly 12,000 to 30,000 dollars; an ISO 27001:2022 Stage 1 plus Stage 2 certification audit runs roughly 14,000 to 38,000. ISO front-loads more work because of its two-stage audit and the required management system, but its renewals are cheaper: years two and three are lighter surveillance audits rather than a fresh report every year.

Does ISO 27001 make me GDPR compliant?
No. ISO 27001 is an information security certification; the GDPR is a data-protection law. Holding ISO 27001 helps you demonstrate the "security of processing" that Article 32 requires, and it is strong evidence of good practice, but it does not by itself make you GDPR compliant and there is no official GDPR certificate you can buy. You still need a lawful basis, data-subject processes, records of processing and the rest of the regulation.

How long is an ISO 27001 certificate valid?
Three years. You earn it through a two-stage initial audit, keep it alive with a shorter surveillance audit in years two and three, and go through a recertification audit before it expires to start a fresh three-year cycle. Note that ISO 27001:2013 is fully retired: the transition deadline was 31 October 2025, so any current certificate is against ISO 27001:2022.

Can I get both SOC 2 and ISO 27001 together?
Yes, and it costs far less than two separate projects because the frameworks share most of their controls. The same evidence does double duty, and one compliance-automation platform covers both. A combined auditor engagement lands around 22,000 to 55,000 dollars, below the roughly 26,000 to 68,000 you would pay for two standalone audits.

Estimate SOC 2 or ISO 27001 cost

Free, no signup: agent.mue.app/tools/soc2-iso27001-readiness-cost-estimator

agent.mue.app/articles/soc2-vs-iso27001-which-a-european-startup-needs