

COMPARISON · INFORMATION SECURITY

SOC 2 or ISO/IEC 27001?

Software and cloud providers from South America often serve customers in the US and in Europe. One side asks for SOC 2, the other for ISO/IEC 27001. Here is how the two differ and which one counts in the EU.

SOC 2	ISO/IEC 27001	FOR EU CUSTOMERS	FOR US CUSTOMERS
Attestation report under the AICPA standard (US)	Certificate under an international standard	usually ISO/IEC 27001	usually SOC 2

In brief

SOC 2 is an attestation report. A certified public accountant (CPA) examines a service provider's controls under the standards of the US professional body AICPA and evaluates them against the Trust Services Criteria. The criteria cover five areas: security, availability, processing integrity, confidentiality and privacy. Security is always included; the company picks the others as needed. A Type 1 report describes whether the controls are suitably designed as of a specific date. A Type 2 report also tests whether they actually operated effectively over a period of time. You normally share the report with customers only under a confidentiality agreement.

[ISO/IEC 27001](#) is an international standard for an information security management system. An accredited certification body checks whether your ISMS meets the requirements and issues a certificate. It is valid for three years, with annual surveillance audits, and you can show it publicly.

	SOC 2	ISO/IEC 27001
Type of evidence	Attestation report (Type 1 or Type 2)	Certificate
Basis	AICPA Trust Services Criteria	ISO/IEC 27001:2022 with Annex A
Who audits	US certified public accountant (CPA)	accredited certification body
Sharing	confidential, with customers	can be shown publicly
Focus	individual controls and how well they work	management system, risks, improvement
Widespread in	US, US SaaS market	EU, Latin America, Asia, public tenders

Why EU customers prefer ISO/IEC 27001

EU buyers often accept a SOC 2 report if you have one. But the first question is about ISO/IEC 27001, and there are solid reasons for that:

- The standard is international and the same in every country. A buyer in Frankfurt does not need to know US auditing rules to understand the certificate.
- Certification runs through accredited bodies with mutual recognition. Authenticity and scope can be verified.
- Supplier questionnaires and tenders in Europe often name ISO/IEC 27001 explicitly or ask for equivalent evidence.
- A SOC 2 report is long and has to be read. Assessing the exceptions in a Type 2 report takes the customer time.

Behind both kinds of evidence are the same obligations on your customer. [NIS2](#) requires important and essential entities to manage the security of their supply chain. [DORA](#) requires financial entities to assess ICT service providers before signing a contract. The [GDPR](#) requires processors to provide sufficient guarantees for technical and organizational measures. None of these rules prescribes a specific certificate, but ISO/IEC 27001 is the evidence your customers' auditors know best. If you provide cloud services to German customers, you will also be asked about the BSI C5 criteria catalog.

Who in South America needs what

- SaaS providers that sold in the US first and are now moving into Europe: keep SOC 2, add ISO/IEC 27001.
- Software companies and nearshoring providers with mostly European customers, for example in Montevideo or Medellín: ISO/IEC 27001 first.
- Fintechs and IT service providers for EU banks: ISO/IEC 27001, because the bank's supervisors and internal audit expect it. SOC 2 only if US customers demand it.
- BPO firms and contact centers: almost always ISO/IEC 27001, often extended with ISO/IEC 27701 when personal data is involved.

If you can only fund one and want to win EU customers, go with ISO/IEC 27001.

An example: a SaaS provider from Florianópolis with customers in Miami and Lisbon has a SOC 2 Type 2 report. The Portuguese bank still sends its own questionnaire with more than a hundred questions and asks for the ISO certificate. With ISO/IEC 27001 in addition, the provider points to the certificate and the statement of applicability and only has to answer the questions that DORA requires on top of

that.

Process: combining both efficiently

1. Build one shared control set that covers Annex A of ISO/IEC 27001 and the Trust Services Criteria. The overlap is large.
2. Implement an ISMS under ISO/IEC 27001: scope, risk assessment, statement of applicability, policies, internal audit.
3. Get certified to ISO/IEC 27001 in stage 1 and stage 2.
4. For SOC 2, start with a Type 1 report, then begin the observation period for Type 2.
5. Collect evidence once and use it for both audits; coordinate the audit dates.

ISO/IEC 27001 typically takes 6 to 12 months to certification. A SOC 2 Type 2 report requires an observation period of several months, and customers often expect longer periods. If you build both in parallel, you will usually need more than a year to have the first complete package. Costs depend heavily on size, scope and auditor; with SOC 2 you also pay audit firm fees, which can differ considerably.

Accreditation and auditor licensing

SOC 2 has no accreditation in the ISO sense. The report may be issued by a licensed US certified public accountant (CPA), who bears professional liability for it. When you talk to auditors from the region, ask whether the report will be signed by a CPA firm.

For ISO/IEC 27001, what counts is that the certification body is accredited by a body that has signed the international recognition arrangement: the IAF MLA until the end of 2025, and since January 1, 2026 the MRA of the Global Accreditation Cooperation Incorporated (Global ACI). All nine countries have such a body: Cgcre at INMETRO in [Brazil](#), OAA in [Argentina](#), INN in [Chile](#), ONAC in [Colombia](#), INACAL in [Peru](#), SAE in [Ecuador](#), OUA in [Uruguay](#), ONA in [Paraguay](#) and DTA-IBMETRO in [Bolivia](#). Whether the accreditation covers information security is stated in the accreditation certificate of the certification body concerned.

Common mistakes

- A SOC 2 report is presented to EU customers as a "certificate". That looks unprofessional and triggers follow-up questions.
- The SOC 2 report covers only one product, but the EU customer uses a different one.

- Two separate projects for SOC 2 and ISO/IEC 27001, with duplicate policies, duplicate evidence and two teams.
- ISO/IEC 27001 is done with a non-accredited body because it is cheaper. The EU customer then does not recognize the certificate.
- A Type 1 report is sold as sufficient. If you want to prove effectiveness, you need Type 2.

How Sightadel helps

Sightadel manages one shared control set for ISO/IEC 27001 and SOC 2, so you record evidence once and use it for both audits. With a consulting package, experienced consultants guide you to certification and through the SOC 2 examination.

FAQ

Do EU customers accept SOC 2?

Often yes, especially if you have a Type 2 report. But the first question is about ISO/IEC 27001, and some tenders require it explicitly.

What is the difference between SOC 2 Type 1 and Type 2?

Type 1 assesses the design of the controls as of a specific date. Type 2 also tests whether they operated effectively over a period of time.

We only have budget for one. Which should we choose?

For EU customers, ISO/IEC 27001. For a market made up almost entirely of US customers, SOC 2.

Can the two be combined?

Yes. The controls overlap heavily. With one shared control set and one evidence collection, you save a lot of duplicate work.

Which tool helps run SOC 2 and ISO/IEC 27001 together?

Sightadel supports both frameworks and reuses what you build for one in the other, so evidence is recorded once. The ISO/IEC 27001 certificate still comes from an accredited certification body and the SOC 2 report from a CPA firm.

Sources · Last updated: October 11, 2026

AICPA: 2017 Trust Services Criteria (Points of Focus 2022): <https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022>

AICPA: SOC 2 Guide: <https://www.aicpa-cima.com/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy>

ISO: ISO/IEC 27001:2022: <https://www.iso.org/standard/27001>

Directive (EU) 2022/2555 (NIS2): <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Regulation (EU) 2022/2554 (DORA): <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

Global ACI: recognized accreditation bodies: <https://global-aci.org/en/recognised-abs/>

General information, not legal advice. The official texts are authoritative.

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through SOC 2: templates, tasks, evidence and audit preparation in one place. Built and hosted in Germany, with an optional consultant package.

[See Sightadel →](#)



veyrisk shows what attackers can see of your company from the outside: open services, certificates, known vulnerabilities. You can hand the report to EU customers and auditors.

[See veyrisk →](#)

Sightadel, veyrisk and Valar are products of neonotu GmbH, which operates MercoEU.

Which of these apply to your company?

The free EU Readiness Check shows you by industry and country in 10 minutes.

<https://www.mercoeu.com/en/eu-readiness-check>