# SOC 2 vs ISO/IEC 27001

## Which Does Your Startup Need?

A practical founder's guide to choosing the right security and compliance path.

**SecureHops**
Security for Startups & Scale-Ups

## The Short Answer

There is no universal winner between SOC 2 and ISO/IEC 27001. The right choice depends on your specific business context.

The right choice depends on:

- Who your customers are
- What customers and procurement teams require
- Where you sell
- Your industry and regulatory environment
- What type of assurance customers expect
- Your security-program maturity
- Whether you need an attestation report, an ISMS certification, or both

### Path A — SOC 2 May Be the Better First Step

- US-focused B2B SaaS
- Enterprise customers explicitly requesting SOC 2
- Customer security questionnaires asking for SOC 2
- Buyers wanting an independent report about controls for a defined service

*SOC 2 is an examination framework based on the AICPA Trust Services Criteria. It produces a report, not a certification.*

### Path B — ISO/IEC 27001 May Be the Better First Step

- International enterprise sales
- Customers specifically requiring ISO/IEC 27001
- Procurement requirements calling for an ISO/IEC 27001 certificate
- Organizations wanting an ISMS-centered information-security management approach
- Situations where formal ISO certification is commercially important

*ISO/IEC 27001 is an international standard specifying requirements for an Information Security Management System (ISMS). Certification is issued by accredited certification bodies.*

### Path C — Both May Make Sense

- The company sells into markets where different buyers request different assurance
- Major customers explicitly require both
- The organization has a mature security program and a business case for maintaining both
- Existing controls, policies, risk management, and evidence can support multiple assurance needs

## Side-by-Side Comparison

| SOC 2 | ISO/IEC 27001 |
| --- | --- |
| **What it is**<br>Examination/report framework based on the AICPA Trust Services Criteria | International standard specifying requirements for an Information Security Management System (ISMS) |
| **Primary framework**<br>AICPA Trust Services Criteria | ISO/IEC 27001:2022 |
| **Developed by**<br>AICPA (American Institute of Certified Public Accountants) | ISO (International Organization for Standardization) |
| **Type of assurance**<br>Attestation report — an independent CPA examines controls | Certification — an accredited body audits the ISMS |
| **Core focus**<br>Controls relevant to a defined system or service | Establishing, implementing, and improving an ISMS |
| **Scope**<br>Defined by the service organization and engagement | Defined by the organization's ISMS boundaries |
| **Buyer question**<br>"Can I see your SOC 2 report?" | "Do you have ISO 27001 certification?" |
| **Evidence expectations**<br>Controls demonstrated during the examination period | ISMS documentation, risk treatment, and operational evidence |
| **Risk management**<br>Relevant to the controls being examined | Central to the ISMS — risk assessment and treatment are core requirements |
| **Terminology**<br>SOC 2 examination, SOC 2 report | ISO/IEC 27001 certification |
| **Best fit**<br>US B2B SaaS with enterprise customers requesting a control attestation report | International sales or customers requiring formal ISMS certification |

## Ask These 7 Questions Before Choosing

1. **What are your next 5–10 enterprise prospects asking for?**
   *The most reliable signal is what your actual buyers request, not what competitors claim.*
2. **Does procurement explicitly require SOC 2, ISO/IEC 27001, or another framework?**
   *Procurement requirements often determine the path more than general market trends.*
3. **Where are your target customers located?**
   *Geographic market affects which assurance format buyers expect.*
4. **What industry or regulatory requirements affect your customers?**
   *Some industries have specific compliance expectations that influence buyer decisions.*
5. **Are you trying to prove controls for a defined service, establish a broader ISMS, or both?**
   *SOC 2 focuses on controls for a defined service. ISO/IEC 27001 establishes an ISMS.*
6. **What security processes and evidence already exist?**
   *Your current maturity level affects which framework is the more practical starting point.*
7. **What assurance will actually help remove a sales blocker?**
   *The goal is practical business value, not collecting frameworks.*

### Do Not Choose Based Only On

- What competitors have
- Which framework sounds more prestigious
- A generic internet recommendation
- An arbitrary startup size
- A generic cost estimate
- A generic timeline

## Decision Matrix

Use this as a starting point. Always confirm customer requirements before committing to a framework.

| Scenario | Potential Starting Point | Why | Verify Before Deciding |
|---|---|---|---|
| **US enterprise SaaS buyers asking for SOC 2** | Consider SOC 2 | Directly addresses buyer request | Confirm actual requirement |
| **International buyers asking for ISO/IEC 27001** | Consider ISO/IEC 27001 | Formal certification may be required | Confirm certification requirement |
| **Mixed customer base** | Evaluate both | Different buyers may need different assurance | Prioritize by sales pipeline impact |
| **Regulated or sensitive industry** | Evaluate both | Regulatory context may affect buyer expectations | Confirm industry-specific requirements |
| **Early startup, no immediate requirement** | May not need either yet | Focus on building security foundations first | Revisit when customer demand appears |
| **Startup receiving repeated questionnaires** | Consider SOC 2 | Questionnaires often signal upcoming requirement | Check which frameworks are requested |
| **Preparing for larger enterprise sales** | Evaluate both | Enterprise buyers often request formal assurance | Confirm buyer expectations |
| **Existing ISO 27001 considering SOC 2** | Consider SOC 2 | Expand assurance for additional buyers | Assess overlap in controls and evidence |
| **Existing SOC 2 considering ISO 27001** | Consider ISO/IEC 27001 | Expand assurance for international buyers | Assess ISMS maturity |

## Can a Startup Do Both?

Yes. An organization can pursue both, but the work should be planned around the actual scope and requirements rather than assuming one automatically satisfies the other.

Both frameworks can involve overlapping security practices:

- Access management
- Risk management
- Policies and documentation
- Security awareness training
- Incident management
- Vendor management
- Change management
- Monitoring and logging
- Evidence collection

*Shared security practices can reduce duplicated effort, but each framework has its own requirements, scope, terminology, assessment or certification process, and evidence expectations.*

### Before Pursuing Both, Confirm

- Scope — What systems, services, and data are in scope for each framework?
- Customer requirements — Which buyers need which assurance, and when?
- Applicable criteria — Which Trust Services Criteria for SOC 2? Which ISO/IEC 27001 clauses apply?
- ISMS boundaries — Where does the ISMS start and end?
- Existing controls — What is already in place that can serve both frameworks?
- Evidence maturity — Can the organization produce evidence for both assurance types?
- Audit or certification strategy — Will examinations or certifications run in parallel or sequentially?
- Internal ownership — Who owns the workstreams for each framework?

## Your Next Step

Don't choose a framework before understanding the gap. The first useful step is usually understanding what the organization already has versus what customers, auditors, or certification bodies will expect.

### A Practical 4-Step Sequence

- 1. Identify customer and market requirements
- 2. Define the relevant scope
- 3. Assess current security and compliance maturity
- 4. Build a prioritized remediation plan

### Not Sure Which Path Fits Your Startup?

Start with a security assessment to understand your current position, identify gaps, and determine the most practical next step.

**Get Your Security Assessment  !'  securehops.com/assessment**
**Book a 30-Min Security Call  !'  securehops.com/book**

## Frequently Asked Questions

**Is SOC 2 the same as ISO 27001?**
No. SOC 2 is an examination framework based on the AICPA Trust Services Criteria that produces an attestation report. ISO/IEC 27001 is an international standard specifying requirements for an ISMS, and certification is issued by accredited bodies. They serve different purposes.

**Is SOC 2 a certification?**
No. SOC 2 produces an attestation report from an independent CPA firm. It is not a certification in the way ISO/IEC 27001 certification works.

**Is ISO 27001 a certification?**
Yes. ISO/IEC 27001 certification is issued by an accredited certification body after auditing the organization's ISMS against the standard's requirements.

**Does a startup need both?**
Not necessarily. The right framework depends on what customers, procurement teams, and market expectations actually require. Some startups benefit from one; others eventually pursue both.

**Which should a startup choose first?**
Start with what your next enterprise customers are asking for. If procurement requests SOC 2, start there. If they require ISO/IEC 27001 certification, start there.

**Can work done for one framework help with the other?**
Yes. Many security practices overlap — access management, risk management, policies, incident response, vendor management, and monitoring. Shared foundations can reduce duplicated effort, but each framework has distinct requirements.

## Sources & Further Reading

**AICPA & CIMA — Trust Services Criteria**
https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
**ISO — ISO/IEC 27001:2022**
https://www.iso.org/standard/27001
**NIST Cybersecurity Framework 2.0**
https://www.nist.gov/cyberframework