SaaS Security
SOC 2 vs. ISO 27001 (or both)
What Every SaaS Firm Needs to Know
Why Even Go for “Provable Security”?

Software-as-a-service (SaaS) firms that serve many industries are often required to acquire/maintain independent validation of their security posture by key stakeholders:

1. Boards and C-suites are demanding “provable security” to reduce business & compliance risk

2. It’s growing increasingly challenging to close a contract unless you are provably secure to an extent that your customers are confident that leveraging your services is not increasing their risk posture. With Personal Information regulations increasing, provable Privacy is the next frontier.
The two “Gold Standards” for independent verification of your information security program are SOC 2 and ISO 27001.

Which should you choose?

Good question let's explore this choice...
Quick Lesson

Do you know the difference between SOC 2 Type 1 vs. Type 2

**SOC 2 Type I (Type 1)**
A SOC 2 Type 1 report attests to the design and documentation of a service provider’s controls and procedures as of a specific date. However, the SOC 2 Type 1 report does not cover the actual operation of the controls. Think of this as a “point-in-time” attestation.

**SOC 2 Type II (Type 2)**
Like a SOC 2 Type 1 report, a SOC 2 Type 2 report covers the design and documentation of controls. A SOC 2 Type 2 report also provides evidence as to how the organization operated its controls over a period of time (usually six months or more). Think of this as a more continuous form of attestation.

We will Focus on SOC 2 Type II
- Here's Your Map -

In our experience, understanding the answers to these questions will determine the best path you should take.

1. What will your clients accept?
2. Which one costs less to prepare for?
3. Which one is faster to achieve?
4. Which costs less to maintain?
5. Which makes you more secure?
6. What is better - ISO 27001 Certificate or Type 2 Service Auditors Report?
7. Which provides more flexibility and more extensibility?
8. Any reason to have both SOC 2 and ISO 27001 attestations?
Question #1
Which one will your clients accept?

The single most important reason to achieve either is to make sure that it satisfies the “ask” from your clients. The good news is that both are widely accepted as most vendor risk management programs specify something like; “… ISO 27001, SOC 2, or equivalent …”

Having done this for nearly 20 years we can guesstimate that there is a:

A 95% chance that an ISO certificate will be accepted (even by someone who prefers/requests SOC 2).

A 90% chance that a SOC 2 Type 2 Report will be accepted (even by someone who prefers ISO 27001.)

The small difference in acceptability relates to ISO 27001 being more widely leveraged internationally. So, if you have a lot of international clients that may be a tipping point.
Question #2
Which one costs less to prepare for?

In terms of overall cost and effort, building your information security program and getting it ready for the attestation audit for ISO 27001 and SOC 2 is pretty comparable.

SOC 2 might be a bit more expensive because the Readiness Assessment (often) costs more than the ISO 27001 Internal Audit.
Question #3
Which one is faster to achieve?

In terms of timeline, building your information security program, and getting it ready for the attestation audit, both are pretty comparable.

- ISO 27001 takes a bit longer to be ready for audit, but the audit can occur immediately after you are ready (certificate in hand for most engagements in 7 - 12 months)

- SOC 2 controls can be fully put into place quicker (2 - 6 months) but a 6 - 12-month observation period is most frequently used in Year 1 so that puts report in hand 8 - 12 months. If having attestation very rapidly is important (& worth the additional cost), you can get a SOC 2 Type 1 attestation when the controls are put in place and then get the SOC 2 Type 2 attestation after a 6-month observation period.
Question #4
Which costs less to maintain?

ISO 27001
In an ISO 27001 audit, the Information Security Management System (ISMS) audit is done to ensure that it’s operating as intended and drives the implementation of the correct Annex A controls to address information security risk. This allows the Annex A technical controls to be audited in a less comprehensive fashion, while still providing comparable assurance.

SOC 2
In a SOC 2 Audit there is no “formal” Management System to audit. SOC 2 provides assurance by a very comprehensive audit of the technical controls specified by the Trust Services Criteria.

These differences make ISO 27001 notably less expensive to maintain relative to SOC 2.
## Example Maintenance Costs

<table>
<thead>
<tr>
<th></th>
<th>ISO 27001</th>
<th>SOC 2 Type 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>$25K - $30K</td>
<td>$40K - $45K</td>
</tr>
<tr>
<td>Year 2</td>
<td>$15K - $20K</td>
<td>$40K - $45K</td>
</tr>
<tr>
<td>Year 3</td>
<td>$15K - $20K</td>
<td>$40K - $45K</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$55K - $70K</strong></td>
<td><strong>$120K - $135K</strong></td>
</tr>
<tr>
<td>Add Privacy Attestation</td>
<td>+ $30K - 45K (3 Yr. Cost)</td>
<td>+ $105K - 120K (3 Yr. Cost)</td>
</tr>
</tbody>
</table>

For a typical small to medium SaaS firm, ISO 27001 costs approximately $60K less over a three-year period.
Question #5: Which makes you more secure?

This is probably the hardest question to answer and likely to draw the most argument. In our (very seasoned) opinion there are four things you should know:

#1 - Assuming optimal implementations...
We would argue that ISO 27001 is the better framework because of its inclusion of a robust ISMS. However, for that to be true, it requires the ISMS, and the ISMS Internal Audit program to be running well.

#2 - SOC 2 has the advantage...
of a more prescriptive and thorough technical controls audit. So, it can be argued that it provides a higher degree of assurance than the technical controls it specifies are running effectively. If we assume that those are the right controls to manage your specific risks, then that would create a high degree of assurance and security.

#3 - Another way to look at...
ISO 27001 gives you a higher degree of assurance that the specified technical controls are the right ones to manage risk while SOC provides a higher degree of assurance that the specified technical controls are operating as intended.

#4 - A more general answer would be...
They both do an excellent job of providing both security and assurance if they are well implemented and well audited.
# Question #6

Which is Better to Give to Your Client, an “ISO 27001 Certificate” or a “Type 2 Service Auditors Report”?

<table>
<thead>
<tr>
<th></th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 2 reports provide a LOT of detail about your security controls</td>
<td>Some think it does a better job of communicating security to your client</td>
<td>Some think it provides more detail than it should. If there are multiple “exceptions” (findings) on a SOC 2 report it might scare your client more than it assures them</td>
</tr>
<tr>
<td>ISO Certificates don’t provide detail about your security controls</td>
<td>Some think that providing detail about your controls is a risk. ISO certificates do not show “nonconformities” (findings) so there is no risk that the certificate may do more harm than good</td>
<td>Some clients may prefer the additional detail that a SOC 2 report provides. There is a workaround for this issue. You can provide a copy of your ISMS Internal Audit (ideally using the Shared Assessments SCA to provide the detail a certificate lacks)</td>
</tr>
</tbody>
</table>
Question #7
Which provides more flexibility and more extensibility?

ISO 27001
ISO 27001 is a member of a large and growing family of information security standards that can be used to address specific use cases (e.g., Cloud Security, Privacy, IT Continuity). You can leverage your ISO 27001 Management System to simplify the operation of other related standards (e.g., ISO-22301 Business Continuity, ISO-20000 IT Service Management). Of significance is the addition of ISO 27701 that extends your ISO 27001 ISMS to concurrently address information security and Privacy. It is the first “certifiable” standard for Privacy.

SOC 2
“SOC 2” usually refers to the Security & Availability Trust principles. You can add up to three additional Trust principles (Processing Integrity, Privacy, and Confidentiality). AICPA offers several other “extensions” including SOC 2 + HITRUST as well as SOC for Cybersecurity. The latter provides a mechanism to communicate relevant and useful information about the effectiveness of your risk management program.

Generally, ISO 27001 provides greater flexibility if you need to address many business/use cases with your cybersecurity program.
Question #8

Any reason to have both SOC 2 and ISO 27001 attestations?
There are three reasons to consider both:

Customer
You have a customer who employs a “checkbox” auditor who insists on you getting the attestation you don’t have. Sometimes this happens and if you want to keep your customer, you do what they ask.

Competitive Advantage
You believe that having ISO 27001 & SOC 2 provides a marketing advantage over your competition. If you appear safer to work with, you may win more business.

Synergy & Efficiency
You recognize that there can be significant synergy between the two frameworks. It could be argued that combining the two creates a “best of both worlds” approach to security. You get the value of an ISMS with the technical auditing rigor of SOC 2.
It's Time to Take The Next Step

Where are you in your journey?

Still Researching SOC 2 & ISO 27001?
Great! We have more resources for you
You can find them here

Evaluating Your Options?
Even better! We have an entire podcast episode dedicated to this topic.
You can find it here

Need to talk to someone... now?
Let's do this! Here is a link to book some time on our SOC 2 experts calendars
Click here!
Getting This Decision Correct is Critical

Not choosing the right attestation can waste a significant amount of time and resources.
But Following Our Plan Will Ensure You Choose Correctly

You have everything you need right here to make the right decision for you!
Any questions? Reach out!

609-581-4600
info@pivotpointsecurity.com