

Test Once, Certify Many

The Multi-Framework Mistake That's Costing You Forty Percent More Than It Should



Summary: Most companies pursuing multiple compliance certifications make one costly mistake: treating each as a separate project. SOC 2, ISO 27001 overlap significantly, yet when different firms run separate engagements, the same controls get tested twice and your team answers the same questions repeatedly. But there's a better way.

If your company is facing simultaneous requirements for a multi-framework compliance audit, such as SOC 2, ISO 27001, PCI, or even just two of the three, there's a very good chance you're about to make an expensive mistake. Not because the certifications are hard. Because almost every company approaches them the wrong way.

The default assumption is that each certification needs its own auditor, its own evidence collection cycle, and its own set of interviews with your control owners. So, you hire a SOC 2 firm, an ISO registrar, and a PCI QSA, and your team spends months answering the same questions three times from three different teams who have never spoken to each other.

But there is a better way. We call it "test once, certify many." And understanding it could cut your combined certification costs by as much as 40-50%, and your team's time burden by significantly more.

Author:

Brett Williams

Risk Advisory and Assurance
Services Leader | Partner

Powell Jones

Partner, Risk Advisory and
Assurance | Information
Assurance

The most expensive mistake in compliance

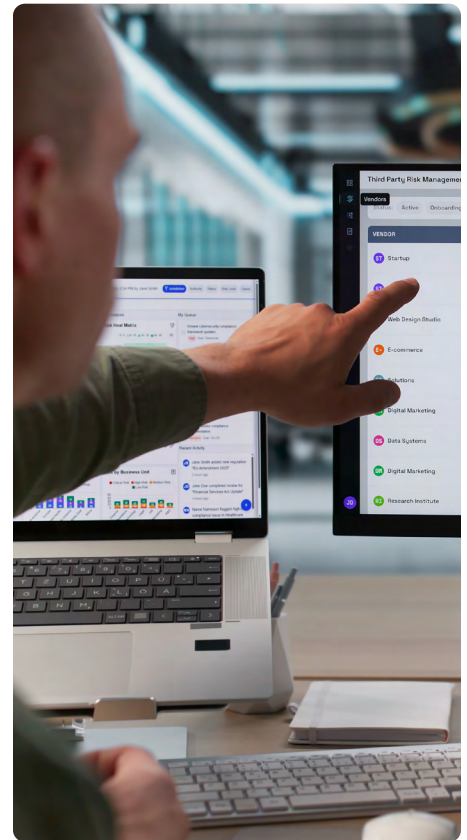
The single most costly mistake a company makes when facing multiple certification requirements is treating each one as a separate project. The frameworks overlap significantly, and in some cases by 50% or more, but when different firms run separate engagements, every overlapping control gets tested twice. Every control owner gets interviewed twice. Every evidence request gets answered twice.

This isn't just a budget problem. It's an operational one. The complaints we hear most often from companies going through multiple certifications simultaneously aren't about cost. They are about their engineering and operations teams being pulled into back-to-back audit meetings for months on end, answering the same change management and access control questions repeatedly from auditors who don't know what the other team already collected.

The problem compounds with every framework you add. SOC 2 plus ISO 27001 is manageable if done separately. Add PCI or CMMC and the redundancy becomes genuinely disruptive.

How much do these frameworks overlap?

More than most buyers realize. Between SOC 2 and ISO 27001, approximately fifty percent of the requirements map across both frameworks. Areas like logical access, onboarding and offboarding, change management, incident response, and backup and recovery are required by both. When we run these engagements together, the overlap typically produces about a forty percent reduction in total audit effort because we're testing the same control once and crediting it to both frameworks rather than testing it independently for each.



What SOC 2 doesn't prepare you for

A company that has completed SOC 2 is well-positioned for ISO 27001, but not fully prepared. The overlapping controls are largely in place and evidenced. What's genuinely new falls into a few specific areas.

Information Security Management System (ISMS)

The most significant addition is ISMS. ISO 27001 requires a structured, documented management system that frames how your organization governs information security. Creating the ISMS in the first year through establishing its scope, objectives, risk treatment process, and management review cycle is work that has no direct SOC 2 equivalent and is frequently underestimated by companies making the transition.

Statement of Applicability

As a related requirement, the Statement of Applicability is a formal document that identifies which Annex A controls apply to your organization, which don't, and why. It's not technically complex, but it requires deliberate attention and someone with enough ISO familiarity to complete it credibly.

ISO 27001

ISO 27001 requires an internal audit before the certifying body performs its assessment. This is not the same as the external audit; it's a structured self-assessment against the standard's requirements, performed by someone with the expertise, to conduct it properly. Most companies outsource this because attempting it internally without ISO-specific knowledge typically results in a longer path to certification, not a shorter one.

The Bottom Line

If your SOC 2 auditor tells you they don't do ISO 27001, that is not a reason to hire a separate ISO firm. It's a reason to reconsider your SOC 2 auditor. In most cases, the time savings alone for your engineering team, your operations team, and your control owners are worth more than the fee reduction. For a lean technology company, time spent in audit meetings is time not spent building product.

- **SOC 2 + ISO 27001:** approximately 40–50% reduction in combined audit fees compared to separate engagements, along with significant reduction in internal team time.
- **Add PCI or CMMC:** an additional 30–40% reduction in incremental fees is possible for the third framework versus treating it as a standalone engagement.
- **Internal time savings:** These are harder to quantify but are often larger than the fee savings. Control owners are interviewed once instead of two or three times, and evidence is pulled once instead of multiple times.

Test once. Certify many. The frameworks are designed to overlap. Your audit engagement should be too.

Policy documentation

Finally, ISO 27001 is more prescriptive about policy documentation than SOC 2. SOC 2 asks whether controls are in place and operating. ISO 27001 expects a documented policy for every significant control area, written to a level of specificity the standard defines. Companies that have SOC 2 policies often find they need to be expanded or restructured to meet ISO requirements, even when the underlying control is identical.

The most common gap we see in companies transitioning from SOC 2 to ISO 27001 is not the controls themselves. It's typically a matter of:

- The ISMS
- The internal audit
- policy depth

Those are the items that require the most lead time and the most external expertise.

Realistic timeline for a dual engagement

For a U.S. company pursuing both SOC 2 and ISO 27001 simultaneously, the realistic timeline to certification depends heavily on whether the ISO-specific groundwork (ISMS, Statement of Applicability, internal audit, and policies) are started early enough.

ISO 27001 certification typically takes nine to 12 months from a standing start. With external support, that timeline can often be reduced to four to six months. Companies that attempt to build the ISO program internally, without a consultant who knows the standard's specific requirements, consistently take longer, not less. The fastest credible path to ISO 27001 certification runs through an experienced external consultant who can build the ISMS, conduct the internal audit, and prepare the documentation concurrently with the SOC 2 audit period.

When both frameworks are running in parallel with an integrated team, the combined timeline is not additive. The SOC 2 audit period, which is a minimum of 90 days, largely determines the shared schedule, while ISO-specific work happens in parallel. The result is that a company can exit a four-to-six-month window with both certifications in hand rather than sequencing them and spending 18 months or more on the combined effort.

Brett Williams leads Risk Advisory & Assurance at Aprio. Powell Jones leads Aprio's ISO practice. Together their teams deliver integrated SOC 2, ISO 27001, PCI, and CMMC engagements for technology companies across the US.

How we can help

With Aprio's comprehensive Risk Advisory and Assurance Services team, you're getting a partner who can help you navigate complex security frameworks, mitigate compliance risks, and enable strategic growth.

[Connect with us](#)