

# Do I Need a GRC Tool for SOC 2?



**Summary:** Not sure if you need a GRC tool for SOC 2? The answer depends on how you use it. GRC platforms help organize evidence and streamline audits, but they don't replace an independent auditor. Learn two mistakes most buyers make, when a GRC tool isn't worth the cost, and how to set one up so it saves time.

Author:

**Brett Williams**

Risk Advisory and Assurance  
Services Leader | Partner

## The GRC tool reality check

If you've already bought a GRC Tool, you may have been told the audit is the easy part. It isn't. And if you're still evaluating whether to buy a governance, risk, and compliance (GRC) tool at all, or whether one replaces the need for a quality auditor, this article is for you too.

The same questions come up whether you're doing your first SOC 2, adding a second framework like ISO 27001, or trying to figure out why your GRC subscription hasn't made compliance feel any simpler.

GRC platforms are valuable tools. But the market has oversold what they can do and undersold what an auditor still has to do regardless of which platform you're running. Understanding that distinction is one of the most important things you can know before you spend a dollar on either.

After performing over 4,000 SOC reports and working with Vanta, Drata, Hyperproof, Sprinto, Secureframe, Anecdotes, Spektrum Labs, here's the practical, no-fluff take.

## What a GRC tool does

A GRC tool is primarily designed to help you organize your evidence, monitor your control environment, and prepare for an audit more efficiently than managing everything manually. The best ones have direct integration with AWS, GitHub, your identity provider,

and other systems that automatically pull the evidence that an auditor needs. When those integrations are set up correctly, they can genuinely save time for both the client and the auditor.

The key phrase here is “set up correctly.”

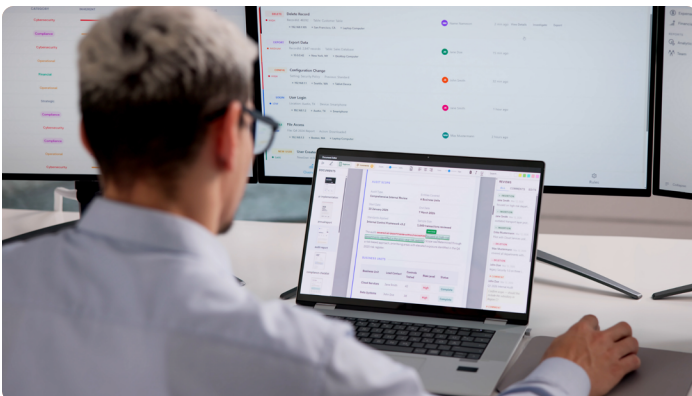
Even with a GRC tool in place, an auditor cannot simply accept the output of those integrations at face value. We still need to verify that the integration was configured properly, that it’s pulling from all the production systems in scope, covering the correct audit period, and returning complete and accurate data. Auditing a GRC tool’s integration output is still an audit. It doesn’t disappear because the evidence came from a platform instead of a spreadsheet. When an audit firm tells you they’ll accept your GRC tool’s evidence without questioning it, that is precisely why the audit industry is developing a bad reputation.

## BYOG: Work with the tool you already have

At Aprio, we refer to this as BYOG, which stands for Bring Your Own GRC. We have formal partnerships with almost every major platform on the market, including Vanta, Drata, Secureframe, Sprinto, Hyperproof, Anecdotes, and Spektrum Labs, among others. We evaluate new tools weekly and regularly audit clients using platforms we’re still formally onboarding, comparing integration output against source systems to verify the tool works before we rely on it.

In practice, this means you don’t have to switch tools, abandon your existing platform, or buy something new before starting an engagement with us. If you’re already working in a particular platform, we probably work in it too. If you’re using something more specialized, we’ll evaluate it. The auditor adapts to the tool, not the other way around.

For smaller companies, typically under 25 people, we’ll often have an honest conversation about whether a GRC tool is necessary at all. At that size, you can frequently walk us through your source systems directly, and the audit can run just as fast or faster without the platform overhead. As organizations grow and more people are involved, integration becomes increasingly valuable. But that calculation is different for every client, and we’d rather help you make the right decision for your situation.



## The two mistakes almost every GRC tool buyer makes

Most companies with a GRC tool fall into one of two camps, and both camps have a problem.

1. **The over-implementer.** This company bought the tool, dove in, and implemented every single control the platform offered, all 150+ of them. This is the point where they need to be gently told that they’ve roughly doubled the scope of their audit. GRC platforms are built to serve every possible company in every possible industry, with controls for scenarios that may have nothing to do with your specific environment. Without an auditor involved from the beginning to define the right scope, you’re testing controls you don’t need. Testing the right 60 or so controls, rather than all 150, is the single biggest time-saver in any SOC 2 engagement, even more so than any integration.
2. **The under-implementer.** This company bought the tool, stored their policies in it, maybe ran the risk assessment module, and called it a day. The integrations were never configured. When audit season arrives, this company looks no different from one that never bought a GRC tool in the first place. They’re essentially paying for an expensive electronic filing cabinet. If the integrations haven’t been implemented, it’s fair to ask why they’re paying for the platform at all, because they’re not getting their money’s worth.

The fix for both problems is the same: bring in your auditor before you configure the tool, not after. That’s exactly how Aprio approaches it.

## What a \$1,500 audit is really telling you

To put it plainly: some companies purchase a GRC tool specifically to get access to the deeply discounted audit firm the platform refers. The math seems to work; a GRC subscription plus a cheap audit still comes in under what a standalone audit costs from a reputable firm. This is not just a GRC tool issue. This is an industry issue.

Recently, a SOC 2 audit covering five trust service categories and over 120 controls was quoted at \$1,500. Even at \$100 an hour, that leaves just 15 hours of work. That is nowhere near enough time to accurately test 120 controls, prepare the report, perform a quality review, and issue a final opinion. It simply is not realistic, and no reputable firm is doing that level of work at that price.

The uncomfortable truth is that a SOC 2 report issued by a firm that did not perform a real audit may pass procurement review at companies that do not know what they're looking at. But any sophisticated buyer, whether a large enterprise, a financial services firm, or a healthcare organization, will recognize immediately what kind of report they have been given.

You get what you pay for. And when the report that's supposed to build trust ends up raising questions instead, the result is not just wasted money, but a liability.

## Final thoughts: So, do you need a GRC tool?

Maybe. Here's how to think about it honestly:

- **If you're a small company with fewer than 25 people and going through your first SOC 2:** you probably don't need one, yet. Start with the audit to gain a much clearer picture of what was difficult and what you need from a tool. That real-world context makes any future GRC tool evaluation far more meaningful than shopping blind.
- **If you're a growing company planning for ongoing compliance:** a GRC tool is worth serious consideration, but only if you commit to implementing the integrations correctly. Otherwise, you're paying for a filing cabinet.
- **If you already have a GRC tool: the first question is whether the integrations are configured.** If not, that's the work that needs to happen before your next audit, and where you can work with your auditor to help you do it right so they can use the output
- **If you're evaluating GRC tools right now: talk to your auditor first.** The right scope and control set should drive your implementation, not the other way around. Implementing the right 60 controls will save you more time than any integration. Also, your auditor can help you identify where to focus for efficient sake, as often testing the source system for certain controls is easier than relying on the output from the GRC tool
- **If you're adding a second certification framework like ISO 27001:** a GRC tool can help you cross-map the two frameworks and manage the overlap between audits. But you also need an audit firm that can handle both certifications and coordinate the fieldwork effectively. The efficiency needs to show up in the audit, not just in the GRC tool's framework mapping.

A GRC tool and a quality auditor are not interchangeable. Each serves different purpose. The tool helps you stay organized and monitors your compliance efforts, while the auditor provides the independent opinion your customers and prospects are looking for. Without the tool, you may be less prepared. Without the right auditor, you may end up with a report that falls short of its value.

**The combination of the tool, if done correctly, is where the value lies.**

*Brett Williams leads Aprio's Risk Advisory and Assurance Services, where he and his team specialize in SOC 1, SOC 2, and SOC 3 examinations. Aprio holds formal partnership relationships with Vanta, Drata, Secureframe, Sprinto, Hyperproof, Anecdotes, and Spektrum Labs, and evaluates new GRC platforms on an ongoing basis.*

## How we can help

Aprio's Risk Advisory and Assurance Services teamwork alongside your GRC platform from day one, helping you scope the right controls, configure your integrations correctly, and walk into your SOC 2 with confidence.

[Connect with us](#)