Don’t Fall For These SOC Reporting Myths | Transcript

Bryan Gayhart & Morgan Hart

August 2026

Morgan Hart: Hey, Bryan, thanks for being here with me today. Today we want to cover some common SOC myths. I've got about 10 here for you.

Bryan Gayhart: I'm ready. Let's do it.

Morgan Hart: All right. Number one, SOC is a certification.

Bryan Gayhart: Yeah, that's a great starting point. We see that a lot. I mean, you can go out on the internet and you can search for that. You can find SOC 2 certification, SOC 1 certification. It's actually an attestation engagement, which at SOC reports, they fall under the AICPA, which then drives the attestation engagement. So as auditors, we're providing an opinion on the design, the implementation, and then the operating effectiveness of the control environment.

So it's not a certification, but we see it all the time when we're talking to prospects, we're talking with clients, when we're talking with report users. A lot of times prospects will say, "Hey, I want to get SOC certified. How long does it take? What's the process?" So then part of it then is educating that it's not a certification. It is that attestation engagement governed by the AICPA.

So we have that conversation, do the education piece, but in practice you'll see a lot. "I need a SOC certification. I want a SOC certification. A customer or a prospect is asking me to get SOC certified." So we just navigate it and you'll even find out in the marketplace where people have made badges or other sorts of things that show, "Hey, I'm SOC certified."

They'll put it on a website, they'll put it in marketing material, et cetera. Not technically correct, but the marketplace, I think, understands what they're getting at at the end of the day. So that's a great starting point. What else you got?

Morgan Hart: Thanks for providing clarity there. Second one I have here is, SOC 1 and SOC 2 are interchangeable.

Bryan Gayhart: Unfortunately they're not. That happens a lot of times in the AICPA, we have a SOC 1, a SOC 2, and then each one has a Type 1 and a Type 2. So as you know, the SOC 1 is driven by financial reporting controls. Think about a payroll provider, a TPA, somebody along those lines. Then a SOC 2 security is the baseline, but then there's other criteria, availability, confidentiality, processing, integrity, privacy, and you can add those in. So they're very different in terms of what they're covering.

So a software company that deals with healthcare records is going to focus more on SOC 2, but a payroll provider is going to focus more on a SOC 1 where it's those controls around financial reporting. So then you get further down into the weeds with the Type 1 and the Type 2, both of those, SOC 1, SOC 2, they each have a Type 1 and a Type 2.

The difference, the Type 1 is just controls in place, point in time. The Type 2 is how well are those controls operating over a period of time? So a lot to digest there. The AICPA, they didn't do us any favors. We have a Type 1, a Type 2, a SOC 1, and a SOC 2. So when you're new and you don't live in the SOC world, that's half the battle is just getting educated on the different types and then finding out which type is most applicable to your company.

Morgan Hart: You mentioned the criteria there a second ago. So in a SOC 2, you have to use all five criteria.

Bryan Gayhart: You do not. So the common criteria, which is the baseline, is security, and that's what drives the majority of SOC reports in the marketplace. Then you can add in availability, confidentiality, processing, integrity, privacy. So what we help our clients with and what we help prospects navigate is if you're pursuing SOC 2, which of those criteria do you need to include? We often tell people, start at the minimum, which is security, the common criteria, and then let your report grow from there.

Then the way it grows is you have customers that ask you, "Hey, I want to see availability." Maybe you have a software application. They want to see availability [inaudible 00:03:49]. Or the other way, if you're going to start with more than just security, it's typically contractual. So you may be working with a bank, a healthcare organization. They may want to see confidentiality, they may want to see privacy. They'll dictate that in their contract with you of what they expect.

Morgan Hart: Got it. Common thing that I've heard across clients of mine and questions in the market are the SOC criteria are prescriptive. What are your thoughts on that?

Bryan Gayhart: Yeah, that's another common myth that's out there. So in the SOC world, if you're focusing on SOC 2, you're looking at criteria, and you need controls in your control environment to meet those criteria. The guidelines established by the AICPA, they don't tell you that you have to have certain controls in place. Or if you come from PCI or you come from HITRUST or other frameworks that are out there, they're more prescriptive.

They may tell you, "Hey, you need to have vulnerability scanning done quarterly. It has to be internal, and it has to be external, but it has to be done quarterly." The SOC world is not that prescriptive. So you end up then with controls in place that represent your company, represent the risk posture that your company has, and then is reflective of what your control environment is and what you want it to be.

So one thing we help our clients navigate is, well, how far down that path do you go? So think vulnerability management, for example. Whatever you put in the report, the system description or internal control procedures, that'll be visible to the end users, the readers of your report. So you have to be comfortable with what you're telling them.

So if you're going to say, "Well, we don't do any vulnerability scan," that's fine. Then that ends up in the report and then the end users are going to see it. So are you comfortable telling them that, and what would their expectation be? So we try to help our clients navigate what the expectations are of the end users of the report so that they can build a control environment that properly flex those expectations.

Morgan Hart: Got it. Thanks for the context there. Another common myth that I hear is that I can do a Type 2 as my first report. What are your thoughts?

Bryan Gayhart: That's a tough one. We hear that a lot, and that's always an interesting conversation. It's not impossible. You can start with a Type 2, so it's not completely a myth, but it is challenging because think of the big lift when you're starting a SOC report. You need controls, and you need to map those controls of the criteria. Then you need to draft the system description.

So those are two parts of kind of coming to the table in the beginning saying, "Hey, we have all this in place. We're going to start with the Type 2. We're confident that our control environment is mature enough and that we're operating our controls as designed." So that's the big risk is if you start with the Type 2, you're running the risk that you may have testing exceptions.

Your system description may not be suitably designed and crafted in such a way that it meets all the criteria. So right out of the gate, you're setting yourself up for potential failure. You could have a qualified opinion, you could have testing exceptions, or if you take a little bit of time and do some readiness, you can identify those gaps and then remediate those gaps and then start the clock on that SOC 2, Type 2.

Then that's the same thing if you're looking at a SOC 1. So you're going to have control objectives around financial reporting, and it's making sure that you have all the controls in place that help you accurately and completely reconcile and record transactions that your end users are relying upon in their financial statements. So in order to do the Type 2 first, you have to be really confident in the maturity of your control plan. Great question.

Morgan Hart: Got it. When looking at a Type 2 engagement, a common myth that I hear is that the period has to be 12 months. Is that true?

Bryan Gayhart: Yeah, that's another common myth that we see. From the AICPA standpoint, as long as the period's at least three months, you can do a Type 2 report. Common in practice is the 12-month report. Then what we try to do and help guide our clients on is identifying what they want that period to cover.

So in a SOC 1, most of the end users are financial statement auditors. So they want something that covers a 12-month period, typically ending in December, because that's most likely when their client has their year-end. So they want maximum coverage over that period of time that they're auditing on the financial statement audit side.

The SOC 2 side is a little different because it doesn't tie into the financial statements. So you have some more flexibility. A lot of times what we'll help clients with is they may have a customer that says, "Hey, we will onboard with you, but only after you have a SOC 2, Type 2." They won't accept the Type 1. So then we'll do readiness, we'll do a Type 1. We'll do that short three month period SOC 2, Type 2 so that they can have that and then give it back to their customer so they can proceed with the onboarding process.

The other thing we'll help our clients do is navigate when that Type 2 period should end because there might be a period of time that's more beneficial for them as a business. Maybe they're slower, April, May, June, July than they are December, January, February. So let's have that SOC 2, Type 2 period end at a time where it's better for the business to allocate resources to getting the report done and getting the report [inaudible 00:08:57], which is important.

Morgan Hart: Yeah, thanks for the insight there. I keep saying this, but another common thing I guess they hear is that a Type 2 is significantly more work. What are your thoughts?

Bryan Gayhart: Yeah, I think that's a common myth, but it can go a couple different ways. If you're going to do the readiness in the Type 1, there's a lot of work on the client side to get prepared. You're putting your policies and procedures together, you're fine-tuning those. Maybe you're adding controls into your control environment. You're doing that control mapping that we talked about earlier. You're drafting that system description.

So there's a lot more work on the client side, I think in the readiness in the Type 1 than in the Type 2. In the Type 2, the client is essentially showing us that, "Hey, we've been operating our control environment over this period of time, and here's the evidence that shows you that." It's all stuff that they've been doing over that 12-month period, we'll say. It's just a matter of gathering those artifacts, sharing those artifacts, and having supporting the evidence available.

Now on the audit side, it becomes more work in the Type 2 because we're testing controls over a period of time. So our audit testing is significantly more involved just due to the volume of work that takes place over that Type 2 period.

Morgan Hart: Sure, that makes sense. Thanks for that. I know within a SOC 1 and a SOC 2, penetration testing can come up as a question often. Is penetration required in the SOC 2?

Bryan Gayhart: Yes, that gets back to one of our earlier questions. That is a common myth that's out there. What you will see is you go back to those SOC 2 criteria and it doesn't anywhere call for penetration testing saying it has to be done. So that gets back to that prescriptive nature of the criteria.

Now you got to think through it if you're a client from a risk standpoint. If I'm a software company, 95% of SOC reports have a penetration test in it. So you most likely want to implement something around penetration testing as a control. You don't have to, but it's a good idea just based on what others are doing from a report standpoint, but it does.

It gets back to the cost benefit. If you're the service organization of how important is it to your control environment? Are your customers going to expect to see that you are doing something like a penetration test every year?

Morgan Hart: A few more items to go through here. Common myth that we hear is anybody can issue a SOC report.

Bryan Gayhart: Yeah, that's definitely a myth. This is a tough one and it's tough in the marketplace. The AICPA, which governs SOC reports, requires that anybody issuing a SOC report be a registered CPA firm. So in the marketplace, you will find a lot of companies out there advertising SOC services, but they're not CPA firms. So then what ends up happening is they can only take you so far where they need to hand you off to a CPA firm. They can then ultimately issue the report.

So if you're the company exploring the SOC report, you think you have this relationship and it's going to issue the SOC report, they can do everything. Well, here comes another third party at the end of the day. Then that third party has to get comfortable with the work that's been done to ultimately issue the report because it's got their opinion in the report.

So the benefit of Barnes Dennig as a CPA firm and a dedicated SOC practice, we do everything from start to finish, whether it's readiness, the Type 1, the Type 2, and then issuing the final report. We don't have to outsource any part of that. Then the other benefit is through the AICPA's peer review program, you can look up Barnes Dennig, you can see our peer review report.

So if you're a buyer of SOC reports, you have an easy way to go check the credibility and the standing of a potential firm that you may be working with, which pays dividends in the end because your end users of the report, the companies that are going to be reading the report, they're going to look for credibility in the CPA firm that's issuing that report. Great question.

Morgan Hart: Definitely. One last item here. SOC reports can be shared publicly.

Bryan Gayhart: That's a myth. We unfortunately see it where people will put the SOC report on their website or the link to it, but they're actually confidential documents to be shared with customers, to be shared with prospects. Most of the time there's an NDA or some sort of agreement to share it.

Now there is a public-facing version of the SOC report. It's the SOC 3, which is not all that common, but you do see it, especially with bigger companies. A lot of large publicly traded companies will have a SOC 3, and that is a public facing document. Think of it as a trimmed down version of the SOC 2 that you can put on your website.

Essentially what that tells you is it gives the user of that report a high-level overview of your company and your operating environment. It doesn't have the controls listed that you typically see in section four, and it doesn't have the auditor testing of those controls. It's just a trimmed down version of the report. So there is a publicly facing version of the SOC report, the SOC 3, but by and large SOC reports are private documents, confidential documents.