Video Name | Transcript

Robert Ramsay, Director, SOC Reporting Practice Leader
Bryan Gayhart, Director, SOC Reporting
May 2025

Robert Ramsay:

Welcome. Hello, I'm Robert Ramsay with Barnes Dennig. Thanks for joining us today for another in our series of SOC discussions. Today, I'm with Bryan Gayhart, a SOC leader here at Barnes Dennig. Bryan, how are you doing today?

Bryan Gayhart:

Very good, thank you. Excited to be here.

Robert Ramsay:

Thanks for joining me. Today, we're talking about SOC 2 Plus. Bryan, when you think of SOC 2 Plus, what comes to mind?

Bryan Gayhart:

For me, SOC 2 Plus is you're adding in another framework. When the SOC report, when you're working off that SOC 2, you're starting with security. That's your baseline. And then, you can add in any of the other criteria, availability, confidentiality, processing, integrity, privacy. But then, SOC 2 Plus is then some other framework that your company is working to meet, working to achieve, so think of things like ISO 27001, NIST 853, things like that. You're going to add that framework into your SOC report. How often do you see that being added in the SOC reports?

Robert Ramsay:

Yeah, that's a good question. I think it's probably between 10% and 20%. It's definitely growing. Five years ago, it was rarer, and now, it's more common. It's nice to be able to add in and get coverage if a company's already living by one of those frameworks, so they can get credit for it without too much effort sometimes if we map to those criteria within the SOC report.

Bryan Gayhart:

Is there one that you see more than others? I know the AICPA provides several mappings, so I assume those are the more popular ones, but are there any frameworks you see more often than not?

Robert Ramsay:

Yeah, that's a good question. I think ISO is increasingly important as the world gets smaller and more companies in Europe do business here and more companies here sell into Europe. We're seeing that as a question quite often.

Bryan Gayhart:

So, let's pick on ISO then. 27001, I know that's a pretty common mapping. There's a lot of overlap for sure, but you can get probably 70% of the way there with the SOC report to cover security, and then you've got to figure out the rest. When you're doing the actual work though, what challenges does that create outside of the normal SOC 2 engagement?

Robert Ramsay:

Yeah, it is a little bit of a challenge. It's also some of the value add is that 30% difference. If they've already got the ISO suite of controls, policies and procedures, what would they need to add for a SOC 2? And the accountants, the AICPA that came up with these have some of their own unique components, and so, we make sure they're in there and we add those into the SOC report, so that it can be SOC 2 Plus ISO.

Bryan Gayhart:

When you're doing that work, where do you put that in the report? Are you putting that cross mapping in the opinion? Are you putting it throughout Section 3, the system description, typically? Do you have separate controls in Section 4 for it? Or, are you just putting it in Section 5 and leaving it alone almost as if it's from management?

Robert Ramsay:

What's nice about the SOC 2 construct that the AICPA came up with is that if it's reasonable and not misleading, there's a lot you can do. I think all those examples you gave, we've probably done some of each in terms of opining on the SOC 2 criteria, noting that that includes some ISO criteria, adding a description of what's going on in Section 3, a disclosure and a report from management, adding controls in Section 4, so that a typical list of maybe SOC 2 controls is longer and more robust. And then, you mentioned Section 5 and mapping just to show that, "Hey, all this work was done, and it is very similar to all this other work that's been done." You can get credit for this in a variety of ways, and so, it's fun doing a lot of different things.

Bryan Gayhart:

In terms of workload, between our workload and the client's workload, where does most of that time fall live? Are we taking on that mapping for our clients? Are the clients taking on that mapping? And then, when it comes to the actual evidence gathering, control testing, where does most of that work reside?

Robert Ramsay:

Yeah. We're in the professional services business, so we're happy to help as much as needed or reduce costs, and some management teams are happy to do quite a bit themselves. We bring to the table CPAs that are independent and trained and certified to issue these reports, and we also can help with preparing the report and pulling this all together. But that said, their team can often do a big chunk of that too, so we work with our clients depending on availability, time, experience, budget, what makes sense for everybody.

Bryan Gayhart:

If you've never done a SOC report before and you have customers and they're asking for a SOC report, they're asking for ISO, it's easy to start and you start with that mapping and the two come together. What about if I've been doing a SOC report for a number of years, and then, all of a sudden I get a customer of mine that says, "Hey, I would like to see ISO 27001." Can we add it in mid-period? Do we add it at the start of the next period? How does that unfold if we'd been doing a SOC report for a number of years?

Robert Ramsay:

Yeah, then the SOC reporting and the testing process is down pat, but adding ISO experience and understanding is the big lift. There's expense to that, joining ISO, paying for the rights to use it. Evaluating the long list of controls and policies, that's typically longer and more involved than a SOC tool, and we can help with that and make that happen.

Bryan Gayhart:

Have you seen any frameworks that any clients have ever asked about that we just can't map to the SOC report, or does everything map?

Robert Ramsay:

One way or another, these are pretty flexible and held to a reasonableness standard. We're able to help with a number of pieces. I know that HECVAT, the Higher Education Cloud Vendor Assessment Tool, has some pieces that are controls that make perfect sense. It has some yes-no questions that maybe you wouldn't call them mapping, but we'd put it in section three as a disclosure item, so we're able to include quite a bit of that.

Bryan Gayhart:

Are there any that we can't map because of different reasons? I think of something like HITRUST, whom we have license. You need to register with HITRUST and basically pay for the use, something like that. Would we be comfortable mapping that or what's it take to map something where there's a paid license in place?

Robert Ramsay:

Yeah. I mentioned I said it before, you've got to pay for that. We do have to play nice with others, and there are intellectual property rights and copyrights and that kind of thing, and they evolve over time. HITRUST changes over time, and so they do have a prescribed method of working with them. And then, there are less prescribed methods that are to be determined.

Bryan Gayhart:

If you're considering one of these SOC 2 paths, any advice for people getting started? Where do you go to figure out if you need it or not?

Robert Ramsay:

Well, whether you need it or not would probably be if your customers care, the readers of these reports. If there's impact and value there, then it's worth going down that path. And like anything else, if you have time to do research in advance, that's great. You can save time and energy. If you're in a huge area and you want an expert to help you, you'll call us sooner than later.

Bryan Gayhart:

We talked a lot about how we help make our client's lives easier. We handle that mapping. We show them that crosswalk. Anything else we do in our process that makes it easier for clients when they're dealing with the SOC 2 Plus?

Robert Ramsay:

We definitely help with best practices, ways that you can get credit for something that's already being done, and in taking the shortest path to the finish line, I know you're really good at that, if something's being done, but it's not quite documented, we'll advise on how you can capture data, so that it can be used in a SOC report, that kind of thing.

Bryan Gayhart:

I'll ask you one last question. Do you have a favorite mapping that exists? I know we see a whole bunch of them. There's a lot of different ones that Cloud Star Alliance, I believe, has this giant crosswalk of mappings that seem to be all-encompassing. Do you have a favorite that you've seen?

Robert Ramsay:

Well, the funniest one is the German one with five long letters to start with Z in English. I'm sure the Germans have a 57-syllable version of that. That's one of my favorites. Most defense forces in the world have their own version. There are many different, kind of quirky. We already mentioned the Higher Education version. They're fun and interesting, depending on who's doing what.

Bryan Gayhart:

Very good. Thank you.

Robert Ramsay:

Yeah. Thank you, Bryan. Thanks for joining us for another video session with Barnes Dennig SOC Team. Call, click or subscribe, and call us with any questions.