SOC Reporting Readiness Assessments & Gap Analysis | Transcript

Robert Ramsay & Bryan Gayhart

June 2025

Robert Ramsay: Hello, thanks for joining us. I'm Robert Ramsay with Barnes Dennig with Bryan Gayhart from our SOC team. Today we're talking about readiness assessments and gap analysis when preparing for SOC reporting. Bryan, you do a lot of these. You're really fast at them. Some of them you do with startups, and some you do with more established companies. Do you have a favorite, or do you look at those very differently?

Bryan Gayhart: I do look at them differently probably. I would say 50% probably of our new clients every year, it's their first SOC report, so that's the immediate question. Most of our new clients, they understand the control environment, they understand IT, they understand the infrastructure of the software, the data, the people, but they don't look at the SOC criteria on a day-to-day basis. So then it's helping them figure out what that gap analysis needs to be and then what that readiness activity looks like.

So if you're a healthcare company and you've been around for 20-plus years, you're probably really mature from a control standpoint, so your gap analysis, your readiness is a lot less involved. But if you're a brand-new startup and you don't even have policies and procedures, then your gap analysis and your readiness assessment gets more involved. So that's what we try to understand on the front end is what that level of effort is. I'll ask you, Robert, in terms of those that you do, where do you tend to start? Do you start with policies and procedures and work from there? Do you start with the criteria and try to go backwards? What's your approach?

Robert Ramsay: For entities that are less mature that haven't had an IT audit of any sort, you do end up starting with policies and trying to identify controls and drafting them and gathering evidence. Nicely for entities that have had another exam of some sort, when we're doing a readiness or a gap assessment, we can use that evidence and go from there on our own asynchronously, take advantage of what's already been gathered, and save management a lot of time.

Bryan Gayhart: That's what I try to do as well. If you've been down the road of PCI or HITRUST or ISO 27001, we want to use what you've already done. We want to make it as

efficient for you as possible. And so that's the first step that I tend to follow. And then if you're just starting from scratch, I try to do a bunch of walkthrough meetings. I want to understand your company and what you already have in place. More often than not, I find that you're doing a lot of great things, you just need to put pen to paper.

And so I want to understand what you're doing. Then we put pen to paper, we help you put your controls together, and then we map them over to the criteria. So that's the approach that I've seen to try to get people to start with what they already have in place. I don't know about you, but my experience is that the readiness and the gap assessment is committing to doing things on a go-forward basis. It's not go hire 10 people, it's not buy some fancy piece of software. Is that what you see when you do it?

Robert Ramsay: Definitely, and one of the nice things, I know our whole team enjoys doing it, you're talking about startups versus more established companies. The established companies, it's sometimes a little easier because they have a lot there already to work with. The startups, we celebrate with them because it's a big deal. It's usually helping them get a new market or a new customer. That's a lot of fun for us to help them achieve something on their goal list. Probably we should talk about the difference between readiness and the gap assessment. Do you think of those as two different things?

Bryan Gayhart: I tend to look at them as very similar, like done in tandem, and then the end result is almost that gap assessment. So back to an earlier example of a healthcare company that's very mature, for them it's more just mapping controls to the criteria. If you're that software startup, it's probably a true element of that gap assessment. You may not have a risk assessment process in place, so we're going to help you figure that out, figure out what looks good for you and what's reasonable, back to what you said earlier. Amazon's risk assessment process is going to be totally different than a two-person startup, and that's ultimately what we're trying to get at is something that is reasonable for their business.

Robert Ramsay: I like the distinction too between the startup and the more mature entity. Startups tend to be quicker on their feet. So if we say, "Hey, there should be this as part of a given policy," they'll change it, and the next day it's in the policy. Those more mature entities, sometimes they need a typed up list of 17 things, and maybe that has to be approved and a plan put together, and then you come back later when the gaps have been addressed. So those gap assessments, sometimes the formal bit tends to be a larger entity. I know sometimes we say our readiness can be like an open book test. We fix it as we go. That's nice with the startups. They work well with that.

Bryan Gayhart: We get a lot of people, I think, that like that model. We call it the crawl-walk-run approach, where you do that readiness, that gap assessment, get your house in order, if you will. And then you do that Type 1 report, if you need it, and then you start the clock on that Type 2 period. And at the end of the day, we're just making sure our clients are set up for success when they do that first Type 2 report, since that's the gold standard, if you will, that people are looking for in terms of assurance from their customers.

Robert Ramsay: It is nice that there's a deliverable at the end of when we do a typical readiness or gap assessment, we're issuing a Type 1 report, and then they have something to show their customers. They get the little blue SOC logo button for their website. That works out well. It gives a full deadline.

Bryan Gayhart: And I think that a little bit of it gets back to our approach. We're not using a cookie cutter or canned approach. We're using those walkthrough meetings to understand your environment. So at the end of the day, we want the controls to reflect your environment. We want the system description to reflect your environment because that's ultimately what the reader is going to get in the report. So we're not trying to fit you in a box. We're not trying to make everybody be on the same playing field. We've got criteria we have to meet, but there's different ways to go about doing it, different ways you can structure your controls to meet those criteria. And I think that's part of our approach, which has been nice, it's unique and then provides maximum value on the back end to the readers.

Robert Ramsay: You're good at that. You're good at helping our customers put their best foot forward in these. I sometimes say you can do anything except be misleading. We do get a lot in there for our clients, and you're really good at that.

Bryan Gayhart: I think the other thing we do is we tend to go a little further on the readiness and the gap assessment. We're getting examples, we're getting evidence along the way that we maybe otherwise wouldn't necessarily need just to issue that Type 1 report. But what that does then is sets the client up for success in the Type 2, where we know what the documentation's going to look like, they know what the documentation that they need to pull is. So we're thinking about the bigger picture even though we're doing the readiness and the gap assessment.

Robert Ramsay: That's a good point. Someone yesterday from a mature enterprise asked me if they could skip the readiness and just go to the Type 2, and I thought they probably did have quite a bit of the controls in place, but I said, "You're more likely to get an A-plus on that Type 2 if we do the readiness, rather than you might get a B or a B-minus if you jump right in and you don't maybe have everything that the AICPA is looking for."

Bryan Gayhart: Yeah, I've seen a fair number of clients start with the SOC Type 2. Some are successful, some aren't, and even those that are, they probably have a really thin report. And then one thing we always do at the end of it is say, "Hey, this is your report. It meets the criteria, all good in terms of the AICPA and what they're looking for, but 99% of SOC reports have these other three controls, five controls, seven controls." Take the pen test for example. You don't have to have a pen test to pass a SOC report or meet the criteria, but 99% of SOC reports have a pen test. So that's the deliverable that is, hey, consider these other controls, these kind of action items for future reports.

Robert Ramsay: That's a good point. Well, this has been great, Bryan. Anything else that we should share related to gap assessments and readiness work?

Bryan Gayhart: I think I'll just add one thing. We really do a lot of this, and we enjoy helping people through this process. As you mentioned earlier, a lot of times that first SOC report has a customer on the back end waiting for it who won't onboard before this report's completed. So we're always willing, always open for conversations. So please don't hesitate to reach out to us. We'd love to talk to you. We'd love to learn about your situation and learn if we can be a great fit to help you out.

Robert Ramsay: That's great, Bryan. Thanks for sharing. That's a good way to close. Thanks for joining us today. Please call, click or subscribe, download our DIY kit, and thank you very much.