DIY SOC Reporting #4 | Which Type of SOC Report Is Right for You? | Video Transcript

Robert Ramsay – CPA, CISA, CITP, HITRUST CCSFP
Bryan Gayhart – CPA, CISA, HITRUST CCSFP

Robert Ramsay:

Hello and welcome to another session of Barnes Denning's Do It Yourself SOC Reporting Readiness Preparation. I'm Robert Ramsey with Barnes Denning and with Brian Gayhart here, another director from our SOC team. Brian, thanks for doing this with me.

Bryan Gayhart:

Yeah, of course. Happy to do it.

Robert Ramsay:

Today we're going to talk about, at a very high level, if someone says you need a SOC report, how do you know which one you need? We've got SOC one and SOC two. We've got type one and type two, and then we also have SOC two with these categories of security, confidentiality, availability, processing, integrity and privacy. And you might wonder what, which one do I do? Brian, how would you answer that question if somebody received a request for a SOC report and didn't know where to start?

Bryan Gayhart:

Yeah, that's a great question. And oftentimes that's the hardest part is getting started is figuring out that SOC one versus the SOC two route and always go back to SOC one centers around financial reporting. So I'm processing transactions for my customer that then impact their financial statements. So their debits and credits that they're recording, they're relying upon my controls in place and my system to make sure that they're getting accurate financial statements. So the debits and credits that flow through. And then you think about the SOC two, so that's more around those trust services criteria that you mentioned. Security, confidentiality, availability, processing, integrity and privacy. So I find those two avenues and then I figure out where I fit in. And then from there you can kind of go down the path of meeting the SOC requirements. Is that how you would start?

Robert Ramsay:

Yeah, that's very good. And then an example, so SOC one is payroll very often because you got to have salary expenses and that's where those come from, your payroll system. And then any cloud-based tool like Slack, which isn't generating debits and credits, but you want to make sure it's secure, they've got a SOC two.

Bryan Gayhart:

Yeah, I think from there then, right? So if you're in the SOC one path, you're working on control objectives. You know that it's around processing a certain type of transaction. But then if you think about the SOC two and the trust services criteria, how do you determine which of those to include? Oftentimes contracts just say, Hey, you need a SOC two, and it doesn't elaborate any further.

Robert Ramsay:

Yeah, that is a good question. I usually try to have a dialogue with our clients about their customers, their contracts and their service. So data centers, security and availability are huge. Sometimes confidentiality and then processing integrity tends to be a category for other. I have a friend who likes to say, "You could do one on popping popcorn if you wanted and you could break down all the steps and you could say we're covering it with processing integrity." And then privacy I usually say is B2C, like business to consumer. So it's a little rarer since so many of these SOC reports are B2B reports, they're business to business and confidentiality's important that these businesses are keeping information confidential, but they don't have consumer data that they're worried about keeping private and certainly a data center isn't dealing with their customer's customer's privacy; they're dealing with confidentiality of their customers. Hope that makes sense.

Bryan Gayhart:

No, that's perfect. And I think it's important then to realize that all SOC two reports include security, that that's the baseline and then the other criteria categories get added on top.

Robert Ramsay:

That's a good point. That's why it's that weird CC nomenclature, which is the common criteria because you have to have it to have any of the others. That's great. Anything else with this whole SOC one and SOC two when you're introducing it to someone?

Bryan Gayhart:

No, I think it just gets back to the contracts and the service being provided and then figure out which path to go down.

Robert Ramsay:

And I guess I can say it again. We've said in other videos. The type one is a simpler report and very often the first one you would issue. So if you were doing a readiness project, your goal would be to issue a whether it's a SOC one, type one or a SOC two, type one, and then subsequently the type twos would happen after a period of time you could test against those controls. Those numbers, we come back to those ones and twos every time and occasionally-

Bryan Gayhart:

Yeah. I think one thing that helps with getting started is probably if you can get it your hands on a report from a competitor, it gives you an idea of what you should be including in your report and what type of report you may need.

Robert Ramsay:

Yeah, that's a good point. Competitors really help because then you can see a lot about how they've decided to describe the environment, which would maybe kind of similar. Another good source is just that entity's vendor. So if they have a payroll provider or a data center or they use Slack, they can go request those SOC reports and have something as a guide to say, oh, I see what this ends up looking like. It's not that hard, is it?

Bryan Gayhart:

Nope. We can get there.

Robert Ramsay:

Right. Awesome. Well, thanks for your time, Bryan. And thanks to everybody who clicked and watched. Reach out, call, click or subscribe. And we're open for questions and ideas for future videos.