BARNES DENNIG
Accounting • Tax • Business Insight

DIY SOC Reporting #6 | SOC Reporting Security Criteria Transcript

Robert Ramsay | Director & SOC Team Practice Leader
Bryan Gayhart | Director, SOC Team
August 2023

Robert Ramsay: Hello, welcome and thanks for joining us for another Barnes Dennig, DIY do-it-yourself, SOC 2 video. Robert Ramsay here with Barnes Dennig. Joining me is Bryan Gayhart. Bryan, thanks for doing this.

Bryan Gayhart: Yeah, no problem. Happy to do it.

Robert Ramsay: So Bryan, it starts at the category level.

Bryan Gayhart: It does. So there's five categories. A SOC 2 report can include security. At a minimum it has to include security, but it can also include availability, confidentiality, processing integrity, and privacy.

Robert Ramsay: Got it. And they used to call it security and now they call it common criteria.

Bryan Gayhart: Exactly. So a lot of times you'll see the CC in front of the criteria number, and that just reflects the common criteria.

Robert Ramsay: Got it. And just further in the weeds, they used to call it principles and now they're categories.

Bryan Gayhart: Correct.

Robert Ramsay: And then the categories are broken down into components.

Bryan Gayhart: Correct.

Robert Ramsay: We're going to try to start diving into the security components, not the disclosure criteria, but the security criteria and how those are provided to us. And they're categorized and labeled and grouped. And we'll talk about different

tiers, those things. What do you think of Bryan, when you think of all those security criteria?

Bryan Gayhart: Yeah, it's a lot to unpack and certainly if you're going through your first SOC report, it can be a challenge. It can be a challenge to figure out how they apply to your business and really where to get started.

Robert Ramsay: We've been doing this for years and we still brought our notes, and our highlighters and our...<glasses> So we're working on this every day. Where should we start?

Bryan Gayhart: So it's probably best to start and just get an understanding, get a lay of the land and figure out how it's all laid out. And it really breaks down into nine components. So these are high level overarching categories. We'll stick to the word components, and it just gives you an idea of what components you need and where you need to go with your SOC report.

And then those components then further break down into criteria. So there's 33 of those criteria, and that gets a little more detailed and gives the user a better understanding of your controls, and your environment. And then underneath those criteria, there's then 208 points of focus. And so that's a lot. 208 points of focus and where you can start that process, but you don't often have to meet all those points of focus, do you?

Robert Ramsay: Right. That's a good point. And that's a good reference to starting the process. It makes a lot of sense to start at that point of focus level, the most detailed level. That'll be a ginormous list of potential controls at your company. And if you meet them, then you can use them in your SOC report. And to your point, they're not required. So you don't have to have every single one of them. They're just a guide to help you see what they meant when they wrote that criteria.

Bryan Gayhart: And they're often a great starting point. It helps with the gap assessment. If you go through it and you can check yes or no, we're doing this, maybe it's not documented, but maybe you're doing it. So that's an easy step. But it allows for you to find out which points of focus you're a little weak on, and then ultimately maybe what criteria you're going to be weak on. And that you'll need to do some gap assessment.

Robert Ramsay: Yep. That's a good way to use it.

Bryan Gayhart: Robert, if I'm getting started on my SOC 2 report and I need some resources, where can I go?

Robert Ramsay: Yeah. Great question. The AICPA sells a big old guidebook, and that's available to you if you want. Freely available is a spreadsheet of all the categories, components, criteria, points of focus, and that spreadsheet's probably... That's where I see most people starting because you can add your own columns, edit, add your notes, share it with your team, and make progress that way.

So you got your book, you got your spreadsheet, you can always reach out to us. We're happy to answer questions, point you to our favorite videos, or help you with any deep type tools that we were able to share. Well, thanks, Bryan. We covered a lot of detailed stuff today. Definitely call us, like, click, subscribe if you need any help whatsoever or ideas for future videos. Good luck with your DIY project. Have a great day.