BARNES DENNIG
Accounting • Tax • Business Insight

How to Read a SOC Report | Ask the Experts | Video Transcript

Robert Ramsay, Director, SOC Reporting Practice Leader
Regina Akrong, SOC Reporting Manager
April 2024

Robert Ramsay (00:10):

Hello, thanks for joining us today, Robert Ramsay and Regina Akrong with Barnes Dennig. Today we're talking about reading SOC reports. So many of the videos we've done have been on our work and what it takes to generate your first SOC report, but today we're going to talk about reading SOC reports. What do you think, Regina?

Regina Akrong (00:28):

I think it's going to be fun.

Robert Ramsay (00:30):

Alright, me too.

Regina Akrong (00:31):

So as a user, let's say I work with an organization that has to request SOC reports. What do I do once I get a SOC report?

Robert Ramsay (00:45):

Yeah, good question. So why are people asking for it and what do they do with it when they get it?

Regina Akrong (00:51):

It's part of our vendor risk management process. So basically we have certain third parties that do stuff for us. Maybe they will send our data to them to process information for us. And as part of the Vendor X management, we have to look at SOC reports. So what do I need to look out for?

Robert Ramsay (01:13):

Yeah, thanks for adding that context. What we've done is we've kind of captured in some checklists things that we recommend folks look for while they're reading these. And I thought I could go through some of that today.

Regina Akrong (01:27):

That would be nice.

Robert Ramsay (01:28):

All right. So as you said, people are often requesting these SOC reports for their key vendors. And then what's funny is there's no green check mark and there's nothing that says pass or fail so that they impose a little work on the reader to know, did I get a good one and is this what I need from it?

And as we were discussing earlier that section three can tell them a lot about the company, so that disclosure portion, they can read about their favorite kind of encryption or what antivirus they're using or how their system is designed and delivered.

Regina Akrong (02:01):

Okay.

Robert Ramsay (02:02):

So that's part of it. But then the reason we have this checklist is because the opinion can be a little hard to read and know exactly whether it's a good report or not a good report, at least in terms of the auditor's perspective. And so yeah, that's what we were thinking. We could talk about some of the things that are included there today.

Regina Akrong (02:21):

So does it help me determine that maybe the third party I'm working with is taking care of my data very well?

Robert Ramsay (02:28):

Yeah, totally. That's a good way to put the big picture of it. Are they doing a good job taking care of your data?

Regina Akrong (02:33):

So what do I start looking at? I mean, I have seen some of the reports and it includes, I know it has a list of controls and the testing performed. So if from an information security point of view, what really do I need to focus on?

Robert Ramsay (02:52):

I think each reader has a different perspective for how much they care about from that information security point of view. So a good point, some of them do care about the type of encryption and antivirus and exactly where their data resides within some cloud vendor and which sector of, maybe it's in the United States, which region it's in, some care about what the sub-service vendors are and what other companies are by this provider of theirs. And so those are listed in there as all the sub-services companies that are critical to the control environment.

Regina Akrong (03:25):

Oh, okay. That's good to know. So for instance, will they help me see if they have very good sign-on procedures and stuff like that?

Robert Ramsay (03:38):

It could be. If that's a part of the service and that's important, then absolutely. The control environment will include sign-on procedures and access requirements and things like that. Some of the other basic things we put on here are just the time period. Is it current or is it a really old report?

Is it applicable to what you need? Some companies will have multiple reports and you want to make sure it's the one for the service you're buying. So that was one of the things like what actually is the scope of this report? Does it include what we're getting from this company? And then as you know, there's SOC one and SOC two, and we've talked about that on other videos, but if you care about internal controls of financial reporting, you want to make sure you're getting a SOC one.

The data security you've talked about is a SOC two, but some of them include availability and confidentiality and some don't. So if that's important, that's another thing to look for.

Regina Akrong (04:32):

Should I be concerned when I see exceptions on the report? Should it be a deal breaker for me, or is it that I can still use the service? I mean, sometimes you don't know whether you want to move on to a new vendor or you just want to stick to whoever you're using.

Robert Ramsay (04:47):

Oh, that's a good question. Yeah, absolutely. I think largely it depends on which control. So if it's one that's very important to you, like the access control you mentioned, if that seems to be failing the tests, then that would be maybe a deal breaker as you said, or a negotiation item where you say, Hey, company, thanks for all you do, but I'd like you to do a little better in this area.

Regina Akrong (05:11):

Okay.

Robert Ramsay (05:11):

That's one way it can be used.

Regina Akrong (05:13):

So if let's say I want to review, I noticed that you provided a document that kind of list stuff that should look out for where would I get access to this if I want to use for my organization?

Robert Ramsay (05:28):

Oh, I'm glad you asked. We make it available. If people reach out to us on the call, click or subscribe to us at Barnes Dennig, we can email it to them. These are just word docs we keep.

Regina Akrong (05:38):

Okay. Robert, I think you answered most of my questions. Nothing comes to mind right now, but maybe let's say that I'm looking at like 20 vendors. I mean, my company relies on so many vendors and I have to do all this every time. Is there a short form I can use? Do I have to fill all this every time? Or you have something that will capture the high-level stuff that I want to focus on?

Robert Ramsay (06:06):

Yeah, that's exactly how we could use this other list. That's a good question. It's a summary, and it could be used to just capture the whole list. It could also be used as a risk basis of doing the long form for your riskier vendors, the ones that have critical data. You could use the shorter form for vendors that are maybe important to the company, but not of super high risk in terms of customer data. That's why we provide two of these.

Regina Akrong (06:35):

Good to know.

Robert Ramsay (06:36):

Good question. Thanks so much for joining me today on the video.

Regina Akrong (06:39):

Thank you. I enjoyed it. You answered my questions and I appreciate it.

Robert Ramsay (06:42):

Oh, you bet. Well, thanks for joining us on our Barnes Dennig SOC video. Call, click, or subscribe and reach out if you'd like copies of the checklists we've talked about, and have a great day.