DIY SOC Reporting #3 | Sub-Service Organizations | Video Transcript

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

Robert Ramsay:

... and welcome to another edition of our Barnes Dennig SOC Readiness Assessment, DIY, do-it-yourself, preparing for SOC reports for those doing one for the first time. I'm with Bryan Gayhart, a director on our SOC team, and today we're talking about sub-service organizations.

How are you doing today, Bryan?

Bryan Gayhart:

I'm very good. How about yourself, Robert?

Robert Ramsay:

Good. Good. Thanks for doing this with me. I was going to start this off with a question just to lay the foundation. What is a sub-service organization?

Bryan Gayhart:

Yeah, definitely, it's a great place to start. They're very critical here in the SOC report because, if you think about your control environment, you've got a whole bunch of vendors that you use. We're all familiar with the vendor phrase, but then, for SOC reports, there's this special vendor which they call a sub-service organization. Essentially, all that is is part of my control environment is relying upon another third party in order to meet the trust services criteria, so whatever I'm trying to it report on. It might be easiest to look at an example, right? If I use a third-party data center, I'm relying on that third party, that data center, to provide physical security controls around that data center. I have a couple options then, right? I can include that in my report in the inclusive method, but that's pretty rare. I mean, do you ever see the inclusive method?

Robert Ramsay:

We do see it typically when they're related parties. There are companies that already own pieces of subsidiaries and they say, oh, go ahead and test them and include them, as you say, the inclusive method, but, by far, 95% of the time, it's that carve-out method.

Bryan Gayhart:

Yeah. When you think about the carve-out method then, I've taken that, we'll stick with the data center example, and I've identified them in my report that, hey, our data is hosted at this data center and my control environment extends to that data center to the extent that they're providing the physical security around where my data is essentially housed if you think about that data center. That's where sub-service organizations come in the SOC report space.

Robert Ramsay:

That's a good way to explain it. Why do readers care? Why do SOC reports own such a special thing called a sub-service org?

Bryan Gayhart:

Yeah. It gets back again to I'm relying upon this service organization for some sort of service, but I want to know who are they using, what are their vendors, what is their key in this process? That's where that sub-service organization comes in. I want to know what third parties they're using. It could be the data center. Maybe a third-party managed service provider is part of the control environment. I want to have a complete picture of the controls at the service organization, so I need to know what those key controls are that they're then outsourcing to these sub-service organizations.

Robert Ramsay:

That's a good way to put it. When I say that a SOC report is half IT audit and half disclosure document, this is that disclosure part where a reader gets to learn about the information and what they're buying when they buy services from this company. Oh, they buy services from a handful of others as well.

Bryan Gayhart:

Yeah. Exactly. If you think about the SOC report process, for us, this is one of the first areas we touch on. You've got to learn about the service organization and the service they're providing, but then it's what vendors, and ultimately these sub-service organizations come into play to help us fully understand that service that they're offering.

Robert Ramsay:

That's great. Do you mind expanding on that? Since this is a DIY concept, would you mind describing the process we go through when we're trying to determine which of these vendors is one of these special vendors, a sub-service org?

Bryan Gayhart:

Yeah. For us, we have this nice spreadsheet that we use, we go through. We identify the key vendors, and we walk through a few steps. We'll look at, do they touch client data? Are they critical to the service offering? If they had a breach, would you have to call your customers? Would you be needing to explain to them that, hey, we outsource a piece. They had an issue. It impacts you. Here's what's happening. We walk through a few steps on how that works and then, ultimately, make a decision. Half the battle is figuring out all the vendors that are in play and then determining if they're sub-service organizations. If you think about the IT space and you think about all the different vendors you may use, that's a starting point. Occasionally, you can go to accounting and say, "Hey, can we get a vendor report of all the people that we pay on a regular basis?" and that might trigger your memory to get a couple others.

Robert Ramsay:

That's right. That happens almost every time. We think of more as we go through the process. Tell me, then once they're identified, what kinds of evidence should someone expect an auditor to show up? Say we show up and say, okay, there are these seven sub-service orgs. What are we going to ask to see, to verify that they've determined as such?

Bryan Gayhart:

Yeah, that's a great question. We carve them out in the report and then we almost point a finger and say, hey, they're responsible for these controls that they need to have them in place, but, at that point, our job is not done as the service organization. We need to then have controls that say, hey, we monitor that sub-service organization to make sure that they're living up to their end of the service level agreement, their contract or whatever services we're getting from them. A common way is to get their SOC report. Read it. Review it. Go back to the data center example. Make sure that the testing around the physical security or whatever else that's important to us at that data center, that they're achieving those controls, there's no exceptions, no issues with their SOC report. If they don't have a SOC report, maybe you have a questionnaire that you send out or even maybe you go visit. Maybe you do a field visit. Not as common anymore, but it's another option.

Robert Ramsay:

Yeah. Yeah. Hey, are there tools that clients can use, that companies can use to monitor their vendors? What do people do to keep track of all that?

Bryan Gayhart:

Yeah, definitely, there's a number of tools out there that we see. A popular one is Venminder. That's one where they'll actually do some work in terms of getting the SOC reports and providing you some information, but it brings together basically a place where you can gather all your documents, you can

do that risk assessment on your vendors, you can track signoffs, things of that sort. OnSpring is another popular one we see. That's more just a place where you do all the work yourself, but it tracks it, allows for approvals, signoffs and notifications of when you need to revisit that vendor.

Robert Ramsay:

Yep. No. Those are great. Thanks very much, Bryan. Here's my curveball question, one more for you. Can the list of sub-service organizations change whether someone is doing a report on security, or security and availability and confidentiality?

Bryan Gayhart:

Yeah. I think it could change. It gets back to what services are being provided. Backups are a lot more critical in terms of availability, and so that may be a sub-service if you're relying on third party to do your backups like a managed service provider. They may be more critical if you're doing availability than if you're just doing security.

Robert Ramsay:

In my experience, that gets proven out when they're matching the precise control that goes to that vendor to make them a sub-service org. Sometimes, those controls are part of the criteria for availability or confidentiality, but not security. In those cases, they end up being added on as sub-service orgs just for certain criteria for that SOC report.

Bryan Gayhart:

Yeah, and I think you'll find that when you do, because you do have to have complementary sub-service organization controls in the report, so that would say, hey, this sub-service is responsible for this control and it meets these criteria so, as you start identifying those, you could then identify different vendors that support availability and confidentiality.

Robert Ramsay:

I'm glad you mentioned that because that does help. When we talk with companies that have started this themselves, if they're really in that gray area, I'm not sure if this is a special vendor sub-service org or just a regular vendor. The proof ends up being, if they can write that sub-service organization control like, all right, what control are we relying on them for and, if they can nail it, then it's clearly a sub-service org. If it ends up being maybe not, then maybe it's a regular vendor.

Bryan Gayhart:

Thanks for the curveball question. I'm not sure if I hit a home run, but maybe I got a single or a double out it.

Robert Ramsay:

You nailed it. Thanks for your time. I think we covered it. I don't know. Is there anything else we should cover?

Bryan Gayhart:

I think we're good.

Robert Ramsay:

All right. Thanks for your time today. That concludes our video on sub-service organizations. If you have any questions for us, call, click or subscribe anytime.