

# Can SOC Audits Be Conducted Remotely? | Video Transcript

Kat Jenkins:

Hi, and welcome to Barnes Dennig Ask the Experts. I'm Kat Jenkins, Marketing Director. And today SOC reporting pros, Robert Ramsay and Bryan Gayhart, talk about the audits for SOC reporting and whether those can be done remotely. Robert and Bryan, thanks for being with us.

Robert Ramsay:

Good morning, Kat. Thanks for doing this with us. Thanks Bryan, thanks for joining me.

Bryan Gayhart:

Yeah, of course, happy to do it.

Robert Ramsay:

We're going to talk about whether SOC reports require in-person visits today. And I think it's kind of interesting, because some standards do and some don't, and some historically companies have expected an annual visit and that's part of the annual nature of these tasks. A lot of audits are like that. But of course, during COVID, it's meant a lot of questioning of travel and onsite visits. So I thought it'd be something to discuss today.

Bryan Gayhart:

Yeah, I think it's a great topic. Especially as I've just come back from the beach and think of how nice the beach is and could I work there permanently? It dawned on me, in terms of, what would I do with my clients? Would I still have to visit them all the time? I don't know if there's an easy answer to this question.

Robert Ramsay:

It is tough. We are guided by reasonableness, so there's variation in practice. One easy answer might be that there's no blanket requirement. So unlike PCI DSS, which for a long time did have that requirement, it's not absolutely required.

Although, because reasonableness is so important and because so many testing requirements may be better in person, things like data centers or anything where physical security is a huge portion of what was being served. So armored vehicles, even casinos, or laboratories with HAZMAT issues. Some of those I could see where you would need to be really careful if you're going to try to get all your evidence without a physical onsite visit. There would be a lot you would need to do.



Bryan Gayhart:

Robert, share with me a little bit about how you handled these visits before COVID, how COVID impacted this, and where you see this going after COVID.

Robert Ramsay:

Yeah. So yeah, historically so much was predicated on a visit. It made sense for relationship building, understanding operations, and then it made it easier to test some things that you could observe in person.

During COVID, of course, with less travel, we've done more Zoom videos and recording and that kind of thing. We've done a little bit more using auditors on-location. An extreme example is Nairobi, Kenya. We have some operations there that we test and we use an auditor there so nobody has to travel to go do that.

And then we use some reasonableness, in terms of planning and saying, "All right, what's the likelihood that their estimation of risk is still valid? That our estimation of risk is still valid? That things haven't changed in the prior year? That the physical controls are operating as expected?" We put a little extra effort into that consideration as well.

Bryan Gayhart:

Does your approach change if a company's environment is all in the cloud versus if they're hosting their own servers on-site?

Robert Ramsay:

Yeah, I'm glad you mentioned that actually, that's a good point. That's the other extreme from those examples I gave where physical security is so important. So many of these SOC 2 reports are cloud-based software as a service companies where all the data is in the cloud. Or even if it's a processor of medical billing and folks are in-person, but all their data is in the cloud, then it's much easier to get comfortable with all the controls needed. And they might be carved out to Google and Amazon and Microsoft such that we don't have to test them actually.

Bryan Gayhart:

Got it. And how does materiality impact all of this when you consider this in your testing?

Robert Ramsay:

Yeah, that's a good point. I think materiality is a slightly technical term that would explain the reasonableness I was describing with all the physical controls at a casino or an armored vehicle company or a lab or a data center. The physical security would be much more material to their customers than it would be to a cloud-based provider. At least our SOC report, if they're going to rely on Amazon's physical security over those servers.

Bryan Gayhart:



And what are you hearing from clients in terms of on-site visit? Is this something they're still expecting to happen? Have they become comfortable with the virtual approach? Is it critical to iron this out in the planning process?

Robert Ramsay:

It is. And nicely, it does improve communication. It's just something that we get to discuss at greater depth. But just like every risk-based decision, these days going to lunch is a risk-based decision, there's a conversation of, "Well, is it worth the travel? Is it worth the visit? On both sides. Is it worth the cost?" And I think everybody appreciates relationship building when it makes sense and appreciates caution when it makes sense. So it seems like it's a day-to-day thing, but yes, it gets more attention and it definitely involves those conversations.

Bryan Gayhart:

Are you seeing anything out there from peer reviewers on this topic or specific guidance in terms of SOC?

Robert Ramsay:

SOC and the AICPA standards have not changed for COVID. Unlike...PCI DSS did, there is some guidance emphasizing the things I've discussed in terms of reasonableness and corroborative inquiry and risk assessment and documenting that and being careful of what you're doing. But no standards have changed and I think it's so far pretty consistent within the industry.

Bryan Gayhart:

Got it. Very good.

Robert Ramsay:

That covers all our questions today.

Bryan Gayhart:

I think it does. That was very informative. And I certainly appreciate that.

Robert Ramsay:

Yeah, thanks for your time.

Kat Jenkins:

Wonderful, great insights. And thank you both so much for being with us today. If you are interested in learning more about SOC reports or need a SOC audit done, then please get in touch with us at [barnesdennig.com](http://barnesdennig.com). We'll see you next time on Ask the Experts.