BARNES DENNIG
Accounting • Tax • Business Insight

SOC Readiness Assessment Ask the Experts Video Transcript

Robert Ramsay, Director, and Kat Jenkins, Marketing Director
Barnes Dennig Ask the Experts July 2020

Kat Jenkins (00:07):

Hello, and welcome to Barnes Dennig Ask the Experts. I'm Kat Jenkins, Marketing Director here at Barnes Dennig. And today I'm talking with Robert Ramsey, Director and Practice Leader for SOC reporting about SOC readiness assessments. Hello, Robert.

Robert Ramsay (00:22):

Hello, Kat. Thanks so much for doing this.

Kat Jenkins (00:24):

My pleasure. Thanks for joining me today. So first of all, tell me what is a readiness assessment? Is it similar to a gap analysis?

Robert Ramsay (00:34):

It is very similar to a gap analysis. It's really the process a company goes through when they're preparing for their first SOC report. We call it a readiness assessment because you're getting ready for that. And the end product is a draft of a SOC report. It includes gathering requirements to be disclosed, controls that meet the criteria. It does depend if it's a SOC 1, or a SOC 2, on whether their control objectives to be determined, and control procedures. In a SOC 1, that's flexible in a SOC 2, it's a prescribed list of security controls, so it's a little more straightforward.

Kat Jenkins (01:13):

And what about a gap analysis?

Robert Ramsay (01:15):

Yeah. Thanks for asking. And then a gap analysis, is a little more of a focus on the gaps or the differences between, where the company is, and where they need to be for a SOC report. So in a formal gap analysis, there's a documentation of the 17 things that aren't there yet that need to be fixed. Sometimes in a large organization, when there's a lot of work to be done around approving changes, that's worth polishing and reporting on and formalizing. Sometimes if a company is more nimble, we're able to fix things and advise as we go along. We find it's often faster to go straight to the finish line if you will, when they're able to do that as we go along. Examples of things would be adding sentences or paragraphs to policies, things that are needed for a SOC report, or asking someone who performs a control on a regular basis to save evidence of that. So if they get an email weekly or monthly, we say, "Please hold onto that. Because we're going to need it later when we test this period."

Kat Jenkins (02:16):

Okay. Does a readiness assessment apply to all levels of SOC reporting?

Robert Ramsay (02:22):

They do. You can do it for a SOC 1 or a SOC 2. SOC 3 is a derivative of SOC 2, so if you can do a SOC 2, you're ready for the SOC 3. And then the type one is the easier version, so it's what we're aiming for. When we do a readiness at the conclusion, you're ready to issue a type one. So it could be a SOC 1, type one or SOC 2, type one. The type two reports take a period of time. So after typically doing a readiness, issuing a type one, in three to 12 months, depending on the timeframe needed we're then ready to issue a type two report.

Kat Jenkins (03:01):

Okay, does a company have to choose during the readiness assessment?

Robert Ramsay (03:07):

They do need to choose whether it's a SOC 1 or a SOC 2, because that guides those controls. The type one and type two is a natural sequence. So they don't really have to worry about that.

Kat Jenkins (03:19):

Okay. And then I know also that there's a wide range of costs for readiness assessment, what drives that?

Robert Ramsay (03:26):

There are. If a company is willing to, or wants to do a lot of this work that can be guided by CPAs, there's a given list of controls and criteria and disclosure requirements that a company can work through on their own just as I say, with a CPA guiding them. Or they can say, "Hey, we're busy enough. You're the experts, here's our policies and procedures. You line it all up and figure out where the gaps are or how ready we are." In which case we're doing most of the work, and so that drives cost.

Kat Jenkins (04:01):

That makes sense. It sounds like too, that companies could save money on a readiness assessment by taking on more of the work themselves. Are there other ways that they could save money during the process?

Robert Ramsay (04:12):

Very much. So another driver is their experience with compliance or policies and procedures. So for example, if they've been PCI-compliant or HIPAA-compliant in the past, they're well-versed in many of these policies and procedures already and it's much smoother. If they're a younger organization, they usually need a little more help in codifying their policies and procedures, formalizing what they're doing. So that drives cost too.

Kat Jenkins (04:41):

Great. So tell me a little bit about what makes a great readiness assessment project.

Robert Ramsay (04:48):

Yeah. The projects go very well when there's a degree of collaboration. So the extent to which we know what the customers want, who are going to read these reports. So the organizations - user entities they're called – we're able to design and guide these reports and answer a lot of the questions. So we know beginning with the end in mind, our team loves collaborating and helping our clients get through these and so they usually go very well.

Kat Jenkins (05:17):

Thank you. Well, that's very helpful. So thanks for sharing information about SOC reporting and readiness assessments with us today. Anything else that people should know?

Robert Ramsay (05:28):

There's a lot they should know, and we're always happy to answer questions. So if they have them, they're welcome to reach out to us through many of the links on our website, call, email, however. There's often a lot of uncertainty, and there's often a chance for the CPAs to help our customers with their end customers determine what kind of report they need and what they want to include in it but we're always happy to help.

Kat Jenkins (05:52):

Fantastic. Thank you. So for more information, please visit us on barnesdennig.com, and we'll see you next time on Ask the Experts.