SOC 2 and SOC 2 Plus Ask the Experts Video Transcript

## Robert Ramsay, DirectorBeth Nelson, Marketing CoordinatorSeptember 2020

Beth Nelson ([00:07](https://www.rev.com/transcript-editor/Edit?token=aqDJmc0L2QdiR_vHGoqfr6TmuvaQJxtD8GtpiLt6j0sexy1C5X5MpYM_w_LCjp42xMgg7B6lACoXqw0zNaU8dL-VQmQ&loadFrom=DocumentDeeplink&ts=7.76)):

Hello, and welcome to Barnes Dennig Ask the Experts. I'm Beth Nelson, and I am the Marketing Communications Coordinator here at Barnes Dennig. And today I'm talking with Robert Ramsay, Director and Practice Leader for SOC Reporting. Hello, Robert.

Robert Ramsay ([00:24](https://www.rev.com/transcript-editor/Edit?token=YFkcVsPtrVtRThgtzN65Vjr0lf3x79gGUpITbqDK7k0VwCn4Hune8kka8ywR05nQq6cvaRKdYYLkXaGIJ8YK4XZ0STo&loadFrom=DocumentDeeplink&ts=24.41)):

Hey, Beth. Thanks for doing this.

Beth Nelson ([00:26](https://www.rev.com/transcript-editor/Edit?token=govm8L_9eApAMIlkrRnXSVYhyp-6nJnw7QaeEcZ9dUxDzGOipyjf6iAEa5_bQXiJ9X7AgAGoxjyZfzdUEZYoOedQkKI&loadFrom=DocumentDeeplink&ts=26.11)):

Well, thank you for joining me. So today we're talking about SOC 2 and SOC 2+. So let's dive in. If SOC 2 is so good, why do they need a Plus?

Robert Ramsay ([00:37](https://www.rev.com/transcript-editor/Edit?token=9UC2L-Jp5cmWleFp0yCVXKWX5ehVmskWvCJKvei5J3mmY38_NPDAja7GWT2hsF-vB_zaN33YYKe5VwZ0gv4RGmp5hvw&loadFrom=DocumentDeeplink&ts=37.92)):

Yeah, thanks that's a good question. The AICPA has developed the SOC 2 using their trust services criteria, and it's their ideas for what makes up a strong control environment for data security. However, there are other groups that have their own opinions about how to list a framework of data security controls. And so there are multiple other groups, international, domestic, by sector and healthcare or others that have their own frameworks. And the AICPA has said, "We're really good at having auditors that are independent, that can test and report things. And so in addition to our trust services criteria, we can test and report on other frameworks." And so that's what they've done and that's what they call a SOC 2+.

Beth Nelson ([01:22](https://www.rev.com/transcript-editor/Edit?token=nUXtzE5xhbQHxxOf_TdhZ_1QctS5dPcyRp7yMF2xMxd67NYz79iYa5yOKGAVJ41Ctb0mGDIp_aeECKLbHkJBtu3s-60&loadFrom=DocumentDeeplink&ts=82.64)):

Okay. So, what are the most popular frameworks that get paired with SOC 2?

Robert Ramsay ([01:29](https://www.rev.com/transcript-editor/Edit?token=Qbs_MSSQfBOHPUCXN8n9MTElexat2mK2KFHoUjbSRmB9c5zFHUpqrAXG1pkX96-_cESlyUxv26NZoluL37r7-sLditY&loadFrom=DocumentDeeplink&ts=89.13)):

Yeah, this is where we get to nerd-out on all my favorite frameworks, and I've even got some notes so I don't take too long with this. But the international body is called ISO, and they have a bunch of their own, but 27,001 is they're leading on information security and their view of the world is that you need a good information security management system, and everything's based on that. So that's if a entity is serving international customers, they're going to ask for ISO, like a SOC 2+ ISO.

Robert Ramsay ([02:00](https://www.rev.com/transcript-editor/Edit?token=hBE6ZaHTv2Y9LNhrux-ehylJ_Bm1zQxwVoeb3ZEPMph9BrQTH__nA0_G403qo2wpJpRMa9yjONWrCWi0XR2X4GfiUr4&loadFrom=DocumentDeeplink&ts=120.14)):

Domestically, in the US, we have something called the National Institute for Standards and Technology, NIST, and they have a bunch of different frameworks for different areas, but they have one for cybersecurity, and it's relatively new and it's exciting for people in my role, in that prior to their framework, the focus was on putting up a huge firewall and keeping all the bad guys out. And their framework is more circular and it says, "Put up a big firewall, keep the bad guys out, but detect the fires and put them out really fast and you should keep doing that all the time." So that's the NIST cybersecurity framework.

Robert Ramsay ([02:36](https://www.rev.com/transcript-editor/Edit?token=qLR9sgrWTVulyCBsnalhvSg98rnWIL190QN83FNzLD3Js-PBfLWQTLdahBTv5oJ4AnEtG3Glle9nK6b4Xdjus-WMOg8&loadFrom=DocumentDeeplink&ts=156.21)):

There's a group called HITRUST in the healthcare space. They were trying to grapple with HIPAA, and they came together with their own list of prescribed tests and controls. And so it's called HITRUST and there's a SOC 2+ HITRUST. There's a group called the STAR Cloud Security Alliance. And STAR is the Security Trust Assurance and Risk framework. And so, if something's in the cloud, they recommend you use their list of controls for specifically cloud-based applications.

Robert Ramsay ([03:07](https://www.rev.com/transcript-editor/Edit?token=ufUNUun4UAS6NXLxpXtQAf7WnEQB-_kWonTYaMSaWdhGDEqvn2qyA6e1JAQDoPx6f0KZyCJhIe5192hKd2PZ1f6ncrc&loadFrom=DocumentDeeplink&ts=187.14)):

So there are loads of these. I'll give a few more of my favorites. In Germany, there's something called C5, and it's Cloud Computing Compliance Controls Catalog. So how's that for alliteration? And I'm sure in German it's one giant word with 100 letters. But the higher education sector in the US has something called HECVAT, they have their own. The Israeli Defense Force has one. But not to be outdone, the US Department of Defense is now, this year they're pushing CMMC, the Cybersecurity Maturity Model Certification, and it applies to all vendors to the Defense Department, whether you're building rockets or just a food vendor. And it nicely, that Maturity Model means that it's more stringent if you're building rockets, and maybe a little less stringent if you're selling food, but either way, you need to be certified to work with the Department of Defense. So there are all these frameworks that a SOC report can include in their reporting.

Beth Nelson ([04:06](https://www.rev.com/transcript-editor/Edit?token=JiIvgrvXZ2Zo4PJLOSvuDk63GeF2-Ra5EAw73y7ro8BdkpY7eojF3uTPZTmZkfAlvC0GVtoSPUDSDHZTtSgrWfiDlcg&loadFrom=DocumentDeeplink&ts=246.45)):

Wow. Well, what are the options for presenting a SOC 2+?

Robert Ramsay ([04:11](https://www.rev.com/transcript-editor/Edit?token=7OCSdTk5Ks-V6Vvx_l2pRlVUYg2PwJhh0PekBwOLHTJtk_o17euZMoR84ffGsGkQoDQgKe0pywM3BXgDTxkGbXVWeRE&loadFrom=DocumentDeeplink&ts=251.75)):

Yeah. So the opinion of the accountants, which is very important to us CPAs, can include an opinion on compliance with those other frameworks, or it can just refer to them and say that management follows them. And the report itself can also disclose all the criteria in those extra frameworks, or it can map The AICPA's criteria to those extra criteria. We call that a mapping. We do that all the time, because as you can imagine, they all have passwords and encryption and antivirus. So 90% of these, quite often, is overlap or the same. And rather than testing them multiple times, we can test once and report on many of these frameworks. And that's where the value comes from these SOC 2s, SOC 2+.

Beth Nelson ([05:00](https://www.rev.com/transcript-editor/Edit?token=1PF99p1secREJMypDO4maVKLM6XPGe3K5kLCIGkPiH2Dlc87uJQ-kLj-QutWrWez3v3cgeA_X9CH0zm3Q5qNhwMuDDk&loadFrom=DocumentDeeplink&ts=300.77)):

Okay. Well, if this is confusing, does your team help straighten this out with your customers' customers?

Robert Ramsay ([05:08](https://www.rev.com/transcript-editor/Edit?token=fLZfMimfMfbrhKynUA36efUK5LTwC0ZW1pC_QTo-qWsrZg9PyN43LUjB9LUt4YTwmFn4ZDEN3NY9rozeRJcVMP353qQ&loadFrom=DocumentDeeplink&ts=308.22)):

Yeah, absolutely. That's a good point because it can be confusing just keeping up with it, let alone the change, so the AICPA changes their rules, and then these bodies like NIST and ISO and HITRUST, they'll change, they have versions, so they change over time. And then, our customers have different contracts with their clients, and they sometimes require a SOC 2 and sometimes require ISO or NIST compliance. And so sometimes we can get involved in those conversations to be very precise about, "Well, how much," I mentioned those different versions of the opinion and whether it's just mapped to the controls, we can be very precise so that everyone knows going in what's needed and we don't do more than is needed, but there's value added to this reporting process.

Beth Nelson ([05:50](https://www.rev.com/transcript-editor/Edit?token=xLKMHL02pxhArYD4cb7G-jCanPgdHTxIPFFUD9NsgM-FCNzTHqXH2uoWDRT_myvgTHX_0UhgfXKsAipMUtEH-VdS2jw&loadFrom=DocumentDeeplink&ts=350.21)):

Oh. Well, thank you Robert for joining us and answering these questions and providing great perspective. So, for more information, please visit us on barnesdennig.com and we'll see you next time on Ask the Experts.