



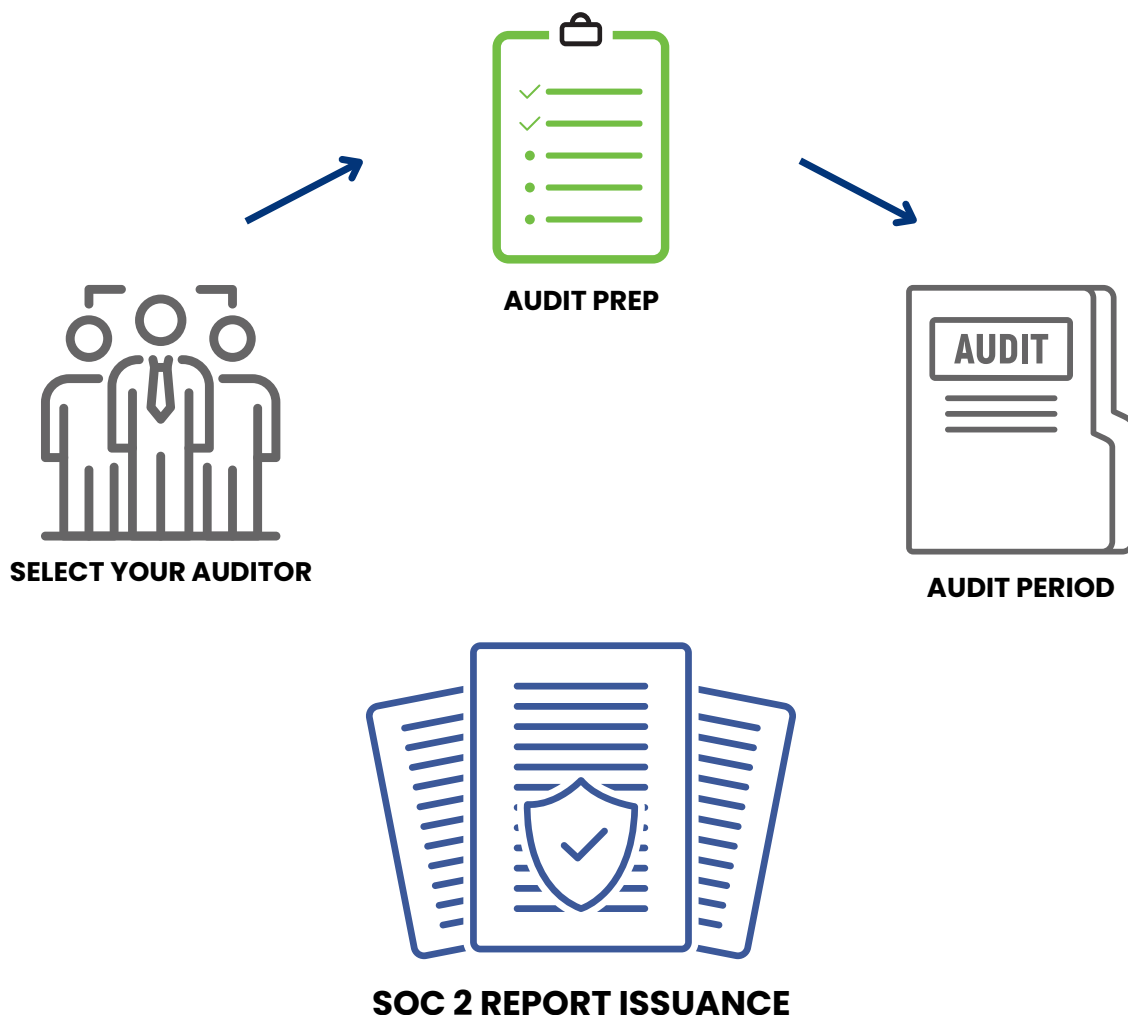
**DANSA
D'ARATA
SOUCIA** LLP

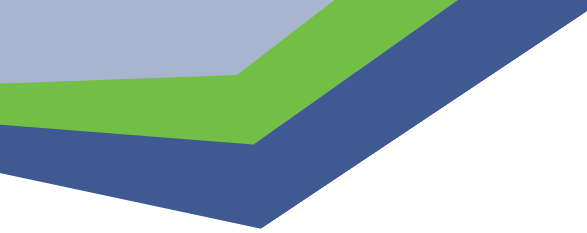
CONSIDERATIONS WHEN SELECTING YOUR SOC 2 AUDITOR

Making Your Selection

What is SOC 2?

System and Organization Controls (SOC) 2 is a framework developed by the American Institute of CPAs (AICPA) in 2011 under the AICPA's Standards for Attestation Engagements (SSAE). This allows independent CPA's a framework in which to report on a Company's internal control design and the operating effectiveness of their controls over data security, system availability, confidentiality, processing integrity and/or privacy. Service organizations that handle, process, and store customer data are the prime candidates to engage in a SOC 2 examination. Boiling it down, a SOC 2 report will help you answer, and give independent third-party verification to the following question: "How can we trust that you will protect our sensitive data and meet the service commitments that you are promising to us?". Not to mention, the completed SOC 2 examination should drastically cut down the number of pesky security questionnaires you are being asked to respond to!





Considerations When Selecting Your SOC 2 Auditor

1 Experience

You will want to work with an experienced firm that has “seen it all”. Experienced firms and auditors will be able to guide you through the process, clearly outlining what you can expect before, during, and after the SOC 2 examination. DDS completes hundreds of SOC 2 examinations each year and is prepared to guide you through this process, from initial project scoping, to clearly articulating expectations. We want to feel like an extension of your team.

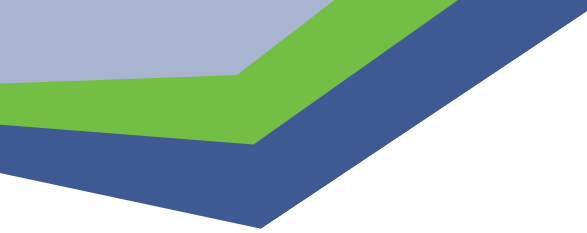
An experienced auditor understands that communication is key. DDS will never leave you wondering where your engagement stands, or how control testing is progressing. We want to build your confidence and remove surprises.

2 Traditional vs. GRC

Over the past few years there have been several Governance, Risk, and Compliance tools (GRC Tools) built to help with SOC 2 readiness and control evidence automation. If using a GRC tool (i.e. Vanta, Drata, TrustCloud, StrikeGraph), you will want your auditor to have experience working with the GRC tool. There are major efficiencies to be gained, but the auditor must know the capabilities and/or limitations of the tool in order to pass along the best cost-benefit to you. DDS has worked through hundreds of engagements using many of the leading GRC tools on the market.

Alternatively, you may decide that a GRC tool is not for you. Maybe you have the in-house expertise to prepare for the SOC 2 and aren't worried about the more manual evidence gathering. You will want an audit firm that is comfortable with requesting and evaluating manual evidence. While most DDS clients these days are utilizing GRC tools, we have plenty of experience with rolling up our sleeves and doing this the old-fashioned way!





3 Customer Base

Are you a start-up or early-stage company? You will want your audit firm to have experience working with smaller, nimble teams. Certain control recommendations do not lend themselves nicely to small teams (think segregation of duties). You will want your auditor to have experience guiding smaller clients around the nuances of meeting the SOC 2 control objectives. While DDS has performed SOC 2 work for clients that have over 1,000 employees, the majority of our clients are smaller teams going through SOC 2 for the first time. This is our bread and butter. We take pride in minimizing the stress and providing clarity to these organizations.

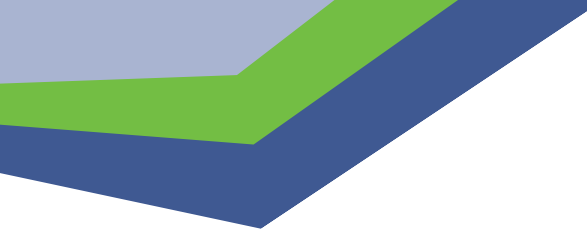
4 Communication

You will want to make sure your auditor is available for frequent questions and check-ins. Whether you prefer to email, setup Zoom calls, or communicate via Skype, your auditor should be prepared to communicate with you and your team how you most feel comfortable.

5 Peer Review

Your auditor should be able to show you their most recent peer review report that covered SOC 2. Firms issuing reports under SSAE standards are supposed to be enrolled in the AICPA's Peer Review Program. During Peer Reviews, an independent CPA reviews both a firm's system of quality control as well as reviews engagements to make sure the engagements are performed and reported on in conformity with applicable professional standards. In the past couple of years as the market demand for SOC 2 has increased, there have been a number of "pop-up" companies offering SOC 2 services. Evaluating their independence and experience is critical. One way to do this is by asking to see the firm's most recently issued peer review report.





6 Independence

CPA firms opining under SSAE standards are required to be independent of their clients both in fact and appearance. The users of your SOC 2 report may take exception if there is any indication that your auditor did not meet independence requirements. While DDS tries to be as helpful as possible, and offer as much insight as possible, we do have some limitations. For instance, we cannot write your policies for you or tell you exactly which controls to implement. GRC tools (which we are independent from) help us maintain our independence by being the unrelated entity that is helping with policy creation, and control recommendations.

7 Timeline/Deadline

When having discussions with potential auditors, you want to ensure that timeline expectations are clearly communicated and are attainable. Discussions surrounding the auditor's process will be important as you need to ensure that timelines will be compatible. For example, any deadlines that you may have for your SOC 2 report should be communicated with your auditor.



The Process of Selecting Your Auditor

You will want to start by having a conversation with all of the audit firms you are interested in. This is your opportunity to ask questions based on the points outlined above to help you determine which firm will be a good fit.

Once you have narrowed down your selection of firms, you may want to vet their reputation. You can do this by asking the firms to provide you with a few references of past clients to reach out to and ask them about their experience.

You may also want to learn more about the team each firm has and who exactly you will be working with for your audit. It may be a good idea to have a meeting with the team member that will be leading your audit specifically.



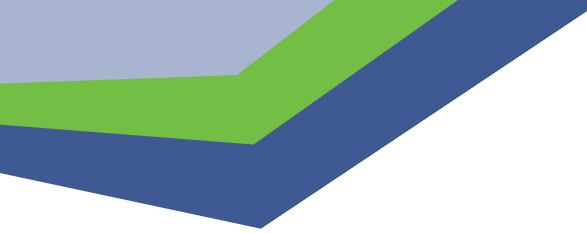
**Interview Potential
Auditors**



**Vet Their
Reputation**



**Meet Your
Audit Team**



Looking to take the next step?

For organizations seeking to undergo a SOC 2 examination, DDS can help! Please reach out to us to discuss any questions you may have and learn about why hundreds of organizations have engaged with us for their SOC 2 attestations.

Reach out to us today utilizing the contact information below to discuss your path to SOC 2!

Contact Us

Dansa D'Arata Soucia LLP is a public accounting and consulting firm focusing on information security attestation and consulting. We offer SOC 1, SOC 2, ISO 27001, GDPR, NIST CSF, HIPAA, and more.

☎ (716) 842-3900

🌐 www.darata.com

✉ mgenson@darata.com

✉ ejacus@darata.com

✉ dgarigen@darata.com

Authors

Madison Genson is a senior information security auditor at Dansa D'Arata Soucia.

Emily Jacus is a senior information security auditor at Dansa D'Arata Soucia.

