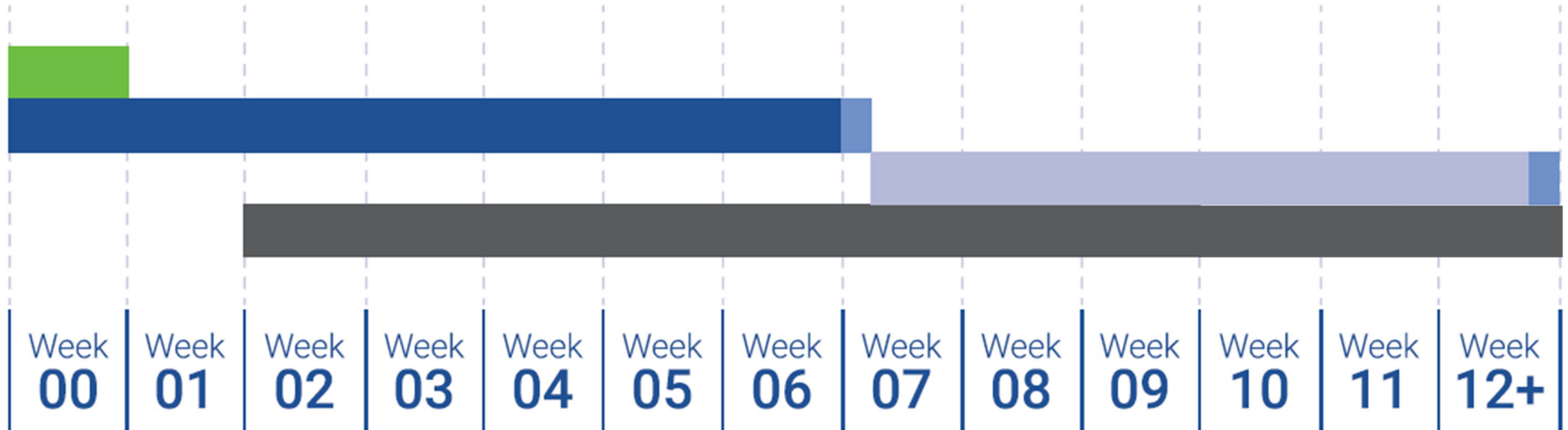


TIMELINE MEASURED IN NUMBERS OF WEEKS



INITIAL DISCUSSIONS & PROJECT SCOPING

- DDS gets to know your unique situation and provides insight on things like:
- a. Type 1 vs. 2 considerations
 - b. Which trust service categories to scope in/out
 - c. Clarity on responsibilities and project timeline
 - d. How we can give you the best chance to SUCCEED
 - e. Working sessions and discussion cadence



REMEDiation PERIOD

- Numerous value-adds:
- a. Expertly trained on Drata platform
 - b. Tips on efficiency and streamlined approach
 - c. DDS takes a collaborative approach while still maintaining "independence"
 - d. Drata system supports remediation steps
 - e. Drata - policy generator, tech integrations, risk based priorities
 - f. Proprietary templates and resources
 - g. Unlimited calls and Q&A sessions
 - h. Sub 24-hour response times
 - i. Goal: YOUR SUCCESS!



TYPE 2 COVERAGE PERIOD

- a. Lasts anywhere from 3 - 12 months (your choice)
- b. Concise instructions provided on how to succeed
- c. Drata automates control tests for high % of controls
- d. Responsibilities clearly articulated
- e. Real time communication of any issues or potential issues
- f. Unlimited calls and Q&A sessions



REPORT WRITING

- a. Control Matrix - DDS builds your control matrix based on the controls you have in place listed in Drata
- b. Part III Management System Description - You write this narrative piece. DDS supports with examples, requirements, etc.
- c. We share with each other, review, and finalize in draft form during the month following the end of the Type 1 or Type 2



ISSUANCE OF FINAL REPORTS

- a. Max of 4 - 6 weeks following Type 1 date or end of Type 2 coverage window
- b. We take a proactive approach to writing and reviewing the reports so that you can receive the report ASAP
- c. DDS provides an attractive reporting package, along with usage instructions, and press release templates
- d. DDS will discuss next steps for follow up SOC 2 reports at this time

Q.) Who is Dansa D'Arata Soucia ("DDS")?

We are a full-service, mid-sized boutique CPA firm founded in 2003 based out of Buffalo, New York. We have become known for our value-add consulting service to complement our technology leveraged approach to traditional compliance work. Our services include but are not limited to SOC 1 and 2 examinations, ISO 27001 internal audits, NIST CSF/800-53/800-171 assessments, and compliance examinations related to regulations such as HIPAA, GDPR and LADMF. In addition, we also offer traditional financial assurance services such as financial statement audits and reviews, corporate and high-net worth tax preparation and consulting, outsourced bookkeeping, controller, and CFO services, business valuations, and transactional consulting.

DDS has performed "SOC work" since the original SAS 70 standard was in place. SAS 70 was eventually replaced by SSAE 16, which created a differentiator between SOC 1 and SOC 2. This was then superseded by SSAE 18, which is the standard currently followed for SOC examinations. In the past couple of years, SOC examinations, specifically SOC 2, which places an emphasis on data security, have gained huge momentum. The absence of SOC 2 is quickly becoming a barrier to entry for service companies in their sales process. Vendor management departments at large organizations are requiring their vendors to have a completed SOC 2 Type 2 before they move forward with a contract.

We can help! DDS has worked closely with Drata on our SOC 2 offerings to provide an incredibly efficient workflow. Drata is an automated security and compliance tool that assists many of our clients with SOC 2 readiness and automates the testing of most SOC 2 relevant controls. Our approach, combined with Drata, creates a SOC 2 examination process that drastically increases your chances of a "clean" SOC 2 report while minimizing the hours needed from your internal resources.

Q.) What is the relationship between DDS and Drata?

We are not Drata and Drata is not DDS. Drata is an IT discovery tool, SOC 2 readiness partner and SOC 2 testing automation platform. DDS is a CPA firm that is qualified to perform and opine on SOC 2 examinations. Drata and DDS have a great working relationship but are separate and distinct from one another. This is an important clarification.

CPA's offering examination opinions must maintain their "independence" from their clients. What this means is that we cannot audit/examine/opine on our own work, whether that be in fact or in appearance. Many companies going through SOC 2 for the first time need a significant amount of direction. This could include a "gap assessment", meaning an identification of where they need to implement additional controls to get through SOC 2, directions on what controls to implement, assistance with policy and procedure writing and formalization, amongst other things. This creates a significant problem for CPA firms trying to service SOC 2 clients. Enter Drata. Drata assists with all these things which provides DDS with the ability to remain independent while still providing plenty of guidance.

Q.) So, DDS is just issuing an opinion?

Not quite. We still view our relationship with our clients as a collaborative effort. Drata creates enough of a distinction between auditor and auditee that it allows us to still offer a significant amount of help in certain situations while still maintaining independence. DDS wants our SOC 2 clients to succeed and puts forth every effort to make that happen.

Q.) What should we be considering in terms of SOC 2 Type 1 vs. SOC 2 Type 2?

Great question. First, let's discuss the difference. A Type 1 is a point in time report and a Type 2 is a report that covers a period of time between 3 months and 12 months. Further, in a Type 1, DDS is only opining on the "design" of your controls as of a particular date. We are not opining on whether or not your controls are operating effectively, i.e., that you are following your policies, etc. During a Type 2, we are performing tests of your controls throughout the coverage period and providing assurance that you are following your policies, that controls remain in place, and that they are operating as they should.

The answer to your original question is that it is almost entirely dependent on what your clients and prospects are asking for. A Type 1 report can get done much quicker and gets product in the hands of your clients/prospects quickly. That being said, anyone asking for a SOC 2 is ultimately going to want to see a Type 2 report because of the additional assurance it provides. The downside of a Type 2 is that there is a minimum coverage period of 3 months, so it takes some time. The downside of doing the Type 1 is that you are incurring a cost for the Type 1 and then immediately starting work on the Type 2 and begin incurring that cost.

Typically, it is our recommendation to see if your clients or prospects are willing to wait for the Type 2 to be completed. In our experiences, most vendor management departments will be understanding of this situation and will be happy enough, knowing that you have engaged an auditor for a SOC 2 Type 2, to move forward with contract even though the SOC 2 Type 2 is months away from completion.

Q.) Got it, so now what about the rest of scoping the project - Which of the 5 Trust Service Categories should be in scope?

The 5 trust service categories are - security, confidentiality, availability, processing integrity, and privacy. Security is the only "must-have". Security is very robust, and we like to describe it as, "Even if all 5 of the TSC were in scope, security would cover 75% of the lift". There is also a fair amount of overlap between security and some of the other categories.

Again, this comes down to what your clients/prospects are asking for. We always recommend asking your clients or prospects what their expectations are before getting too far into the project.

We have a significant amount of resources we can share that dive into each of these categories further, but a general overview of each is as follows,

- Security - Your systems and data are protected against unauthorized access.
- Confidentiality - Confidential information is protected.
- Availability - Systems and processes are available and operational 99.9999% of the time.
- Processing Integrity - System processing is complete, accurate, valid, and timely.
- Privacy - PII is collected, used, retained, disclosed, and disposed of in accordance with policies.

It is worth noting that security covers much more than just access controls as the above note suggests. Security is also referred to as the common criteria. There are many criteria that would be shared amongst many of the categories. Rather than be repetitive, these have all been included under security. For instance, Risk Assessment controls would be important to all 5 categories. Rather than reiterating controls, the framework includes Risk Assessment controls under security. It is very common for a SOC 2 engagement to only include the security category.

Q.) What controls do we need to have in place?

We always recommend that we are engaged as early as possible in the process. We do a significant amount of our work before your Type 1 date, or before the start of your Type 2 coverage period. Drata has created a VERY robust platform, but no company is likely to have all controls that Drata suggests implemented. We can help direct your focus to controls that will matter for you.

Other control frameworks state "here are 100 controls, you need to have all of these in place". SOC 2 is different. SOC 2 has pre-determined control objectives but leaves it up to the company to show how they solve each objective through control design and implementation. As such, there is quite a bit of flexibility. Our goal during remediation is to make sure that it appears that you will have enough coverage with your controls so that all objectives are met.

Q.) OK, so talk to me about the remediation process:

Once we are formally engaged, we get read-only access to your Drata instance. From there we give you a bit of time to work on integrating your tech stack with Drata, generating policies using Drata's policy generator, getting employees to sign-off on policies etc. Basically, make some significant progress. During this we are, of course, available for any questions you have as frequently as you have them. Once you have made some progress, we will schedule our first "working session". This will be via Zoom or another video conferencing platform so that we can screen share and look through your Drata instance together. From there you will be left with some actionable items to work on. In the meantime, if we haven't already, we will start building out your control matrix.

This becomes part of your SOC 2 reporting package. This is a list of controls that we see you have in place (either from just looking at Drata or from other conversations that we have had). We align the controls with the control objectives. The goal here is to make certain that you have coverage for each objective. As our first working session wraps up, we will set a cadence for additional calls or working sessions leading up to your Type 1 date or start of Type 2 coverage period ("start date").

The most critical call is approximately 7-10 days before the start date. By that call you should feel like you have mostly everything remediated and in place. This call will be a final check-in to make sure everything looks good heading into the start date. Any gaps will be discussed, and you will still have 7-10 days to solve for any open items.

Q.) You mentioned you work on the Control Matrix. I am scared to ask. Who writes the narrative (aka System Description)?

Awkward...sorry...you do. Back to the independence issue. We not only opine on your controls, but also opine on the fairness of the information in the narrative. As such, this must come from you in version 1. Now, I do have good news. We do all we can to help. We offer plenty of resources to make this as painless as possible (as does Drata). We have recommended structure templates, checklists to make sure everything required is discussed, and even some name-redacted examples we share with you. It really is not too much of a burden. Additionally, it gives you a great chance to show off!

Q.) I think I get it so far. What about the coverage period?

So far, we have gone over what the process is to make sure your controls are designed appropriately. Now, how do you prove to us that they are operating effectively over the Type 2 coverage window? In those 7-10 days before the start of your coverage period we put together a comprehensive list of expectations based on your unique controls for during the coverage period.

Your main directive during the coverage period is to make sure everything in Drata remains “clean”. By “clean” we mean as close to 100% passing as possible. I’m sure your next question is “What if something does fail”? Do not worry, there are very few cases where 100% of your controls will be passing 100% of the time. The great thing is, if a control does fail, Drata provides detailed logs of what caused the failure, and most of the time we are able to sort things out, i.e., an asset was added that is not in scope, an account was added that is “not a person”, the failure was a “bug”, we have seen it all! We will make every effort to rectify the failure before we even begin the process of reporting the failure in the report.

Q.) Sell me on Drata and DDS, what makes you different?

Thanks for asking. I will start with Drata. Drata has built an extremely user friendly and comprehensive platform. They also dedicate a ton of time to training auditors like us on the platform and taking auditor suggestions regarding continuous improvement of the platform to heart. They are uber focused on streamlining and simplifying the SOC 2 process. Their platform provides a clear roadmap to compliance and automates a huge number of tasks. From flagging tasks based on importance, to providing layman's directions on how to remediate each failing task, to taking a Q&A approach to generating SOC 2 compliant policies, to alarming you when any passing controls fall into a failing state, Drata has your success as their first priority.

The benefits to using Drata are numerous, I could go on for pages. But enough about them, let us talk about DDS. We have spent countless hours working towards perfecting our SOC 2 process specific to companies using Drata and DDS as a combination approach to SOC 2. We have dozens of resources to share with you to make your life as easy as possible throughout the SOC 2 experience. Most importantly, we specialize in SOC 2 examinations for companies your size. Certain firms are better suited to perform SOC 2 examinations for large organizations. We specialize in small to medium size organizations. Why? Typically, these companies are going through SOC 2 for the first time.

We get that these companies need the personal touch and assistance that we can offer. Sure, we maintain our independence and have other standards to follow but that does not mean that we cannot take an approach to this that makes us feel like a partner of yours!

Please do not hesitate to ask us further questions. We are always willing to add to this list!

On behalf of Dansa D'Arata Soucia LLP,



Daniel R. Garigen, CPA

Partner

dgarigen@darata.com



Taylor L. Gavigan, CPA, CISA, CITP

Manager

tgavigan@darata.com