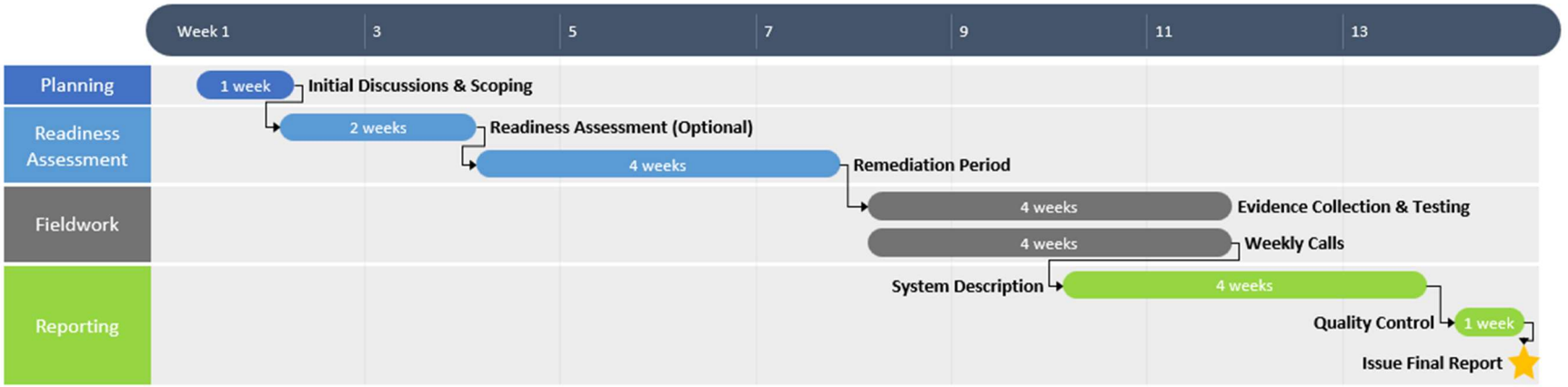
PEASE BELL CPAs

SOC 2 Timeline



Planning	Readiness Assessment	Fieldwork	Reporting	Issuance of Final Report
Pease Bell CPAs asks questions and <u>listens.</u> a. Purpose for SOC 2 b. Data types you encounter. c. Tech stack d. Which Trust Service Categories to scope in/out e. Clarity on responsibilities and project timeline	Optional "kicking the tires" assessment. a. Review current state of policies, procedures, and operations. b. Provide Gap Report and recommendations for remediation. c. Tips on efficiency and streamlined approach. d. PB takes a consultative approach while maintaining "independence." e. Proprietary templates and resources f. Unlimited calls and Q&A sessions	a. Project timeline communicated to assign responsibilities and hold both parties accountable. b. Drata automates a high % of evidence collection and control performance c. Recurring meetings for real time communication, questions, and addressing potential issues. d. Concise instructions for how to succeed	a. Section 3: Management's System Description – you write this narrative piece. PB will provide support with examples, requirements, and templates. b. Max 2 weeks from the last piece of evidence provided, you will have a draft report in hand for review. c. Engagement quality control reviews all reports for adherence to reporting requirements	a. Final report issued within 48 hours of your final sign-off. b. Final report issued along with usage instructions, press release templates, and a list of our recommendations. c. Discuss next steps for continued compliance and future reports

CLEVELAND
1111 Superior Ave E, Suite 2500
Cleveland, OH 44114 | P: 216.348.9600

AKRON
3501 Embassy Pkwy, Suite 200
Akron, OH 44333 | P: 330.666.4199

NEW JERSEY
411 Boulevard of the Americas, Suite 503
Lakewood, NJ 08701 | P: 216.348.9600

Who is Pease Bell CPAs LLC?

"Pease Bell" is a full-service CPA firm, headquartered in Cleveland, Oh with offices in Fairlawn, OH and Lakewood, NJ. With over 170 employees, our areas of expertise include information security attestation and consulting (SOC 1, SOC 2, ISO internal audit, GDPR, HIPAA, and others), traditional compliance services (taxation and financial statement assurance), transaction services (buy side diligence and quality of earnings), client accounting services (outsourced bookkeeping, controller, CFO), and more!

Pease Bell's Risk Advisory specialists understand the growing need for IT & IS assurance and compliance services. The Risk Advisory team looks to educate and support our clients; focusing on solution-based practices for clients seeking to comply or in the process of becoming compliant. We carefully dissect each aspect of our clients' business operations to create a strategic, tailored solution to meet one or many of their compliance needs.

Our goal is to simplify and expedite the compliance reporting process to meet the stringent demands their customers, vendors and governing bodies require. This is why we have maintained a relationship with Drata since the formation of our Risk Advisory Services group in 2020! Drata offers our clients with great resources and an efficient way to collect evidence and maintain compliance.

What is the relationship between Pease Bell CPAs and Drata?

Drata and Pease Bell have a mutually beneficial relationship. Drata is a Governance, Risk, and Compliance (GRC) platform that a client uses as an IT discovery tool, SOC 2 readiness partner and SOC 2 testing automation platform. Pease Bell is a CPA firm that provides SOC 2 reporting services (in addition to audit, tax, and bookkeeping services). Explained another way, if the SOC 2 process is a four-step process, Drata helps a client through steps 1 and 2 (readiness and evidence collection) and Pease Bell helps a client through steps 3 and 4 (testing and reporting). The Drata and Pease Bell relationship offers unique benefits for both the client and Pease Bell. Drata offers the client great resources for identifying gaps and remediating those gaps with templates and consulting. Pease Bell benefits from obtaining access to relevant and timely evidence from the automated evidence collection tool within Drata.

Why doesn't; Pease Bell do all 4 steps? You might ask. We would love to but as a CPA we have to remain independent from the implementation and performance of controls if we are to audit those controls.

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

The audit process is mostly the same whether you are striving for a SOC 2 Type 1 or a SOC 2 Type 2 however, the level of assurance and examination period are quite different. A Type 1 is a measure of your control activities design and implementation, meaning is the control in place or not. To test for control implementation, we will inspect a sample of one (ex. one new hire checklist for a recently hired employee). Each Type 1 report has an "as of" date meaning the controls included in the report were designed and in place as of this date. It marks the point in time or cut-off period for the audit.

A Type 2 is a measure of your control activities implementation (same as a Type 1) and operating effectiveness. Operating effectiveness is measured by how well or how consistent the control was performed. To test operating effectiveness, we will inspect a sample of 10% of the total population (ex. If you hired 100 employees, we would inspect 10 new hire checklists). Each Type 2 report has an examination period or the period under review. Examination periods are somewhere between 3-12 months long and depending on your contractual requirements, we can help you decide what examination period makes the most sense.

The answer to your original question is that it is almost entirely dependent on what your clients and prospects are asking for. Both have their advantages and disadvantages. A Type 1 report takes much less time to complete, and you can achieve a quick win by putting a product in the hands of your clients/prospects quickly. However, usually any contractual requirements for a SOC 2 ultimately require a Type 2 because of the added assurance it provides. So, you may be able to celebrate the completion of the Type 1 but then need to

incur the time and cost of immediately starting your Type 2. The end goal is to complete an annual Type 2 report. However, the minimum coverage period is 3 months, so it takes time.

Typically, it is our recommendation to see if your clients or prospects are willing to accept a Type 1 report for year 1 with the plans to complete a 12-month Type 2 report starting the day after the Type 1 report was issued. This allows you to see the SOC 2 audit process, quickly obtain a report to pass along to your clients or prospects and spread the cost of 2 SOC 2 reports over 2 different annual budgets. 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.

What are these Trust Service Categories and which ones should we include in scope?

The 5 trust service categories are security, availability, confidentiality, processing integrity, and privacy. The security category is the foundation for the SOC 2 and is required to be included in scope. The other 4 categories are more or less optional however we will ask specific questions in our planning phase to help determine which categories make the most sense to include (and we will check to see what your clients and prospects would expect to see in the report). Below is a brief summary of each category:

Security – operational, logical, and physical security controls are in place to protect your systems and data.
Availability – operations and data are available 99% of the time.
Confidentiality – confidential information is protected and stored (and disposed of) according to retention periods.
Processing Integrity – system processing is complete, accurate, and timely.
Privacy – PII is collected, used, retained, disclosed and disposed of in accordance with your policies.

So, do you send us a list of controls we have to implement to meet the Trust Service Categories?

Not exactly. Drata will provide you with a list of controls but each client is unique and the controls will need tailoring. Once we are formally engaged, we will receive read-only access to your Drata Portal. We will review your current progress in Drata and request our first working session. This will be via Teams meeting or other video conferencing platform so we can ask questions about your operations and control performance. Our goal is to either adjust the control language to meet your operations and/or communicate the evidence task so you know exactly what to provide us with. At the conclusion of the working session, you as the client and us as the auditor will have clear actionable items to address prior to our next working session. These working sessions will help fine-tune your custom list of control that will be presented in your SOC 2 report.

What about the Readiness Assessment?

This is an optional step in our process. If you have never been through SOC 2 reporting before and you want to see how you stack up against the criteria, this is for you. We will do a 2-week assessment looking at controls and evidence from a high level to determine a readiness score and Gap Report. The Gap Report will detail the areas that you need to implement or remediate certain controls. We will offer our recommendation on how to best remediate each control (and depending on the control we will make referrals to our trusted third parties to help you in the process).

The readiness assessment is for internal purposes only, meaning you will not have anything to share with your clients and prospects. But you will have a clear roadmap to a successful SOC 2 Type 1 or Type 2.

The timeline makes sense but what is a System Description and who writes it?

A System Description is a term used by the AICPA and it is basically a narrative of your policies, procedures, people, data, infrastructure, etc. used to deliver your services to your clients. Still confused? We offer plenty of resources to make this as painless

as possible. We have templates to serve as a starting spot, checklists to make sure everything required is mentioned, and even some name-redacted examples we share with you. With our support, this is not a super heavy lift. Plus, it is a great opportunity for you to brag about your company!

Why should we choose Pease Bell?

We are focused on efficiency and effective communication. We understand you are not going through a compliance audit for the fun of it. In our opinion, efficiency is key in providing a great client service experience when it comes to compliance audits. Our managers are trained to anticipate your questions and needs and answer them before you ask. We take great pride in our storytelling abilities and will help you understand exactly what you need to do to meet or exceed the compliance regulations.

We have dozens of templates and resources to share with you to make your life as easy as possible. We get the most satisfaction from providing our services to small and mid-sized companies. For many of our clients, this is the first time they have had to show compliance with SOC 2. We understand that you may need the personal touch or assistance to get across the finish line. Yes, we have to remain independent from implementing or performing your controls but that does not mean we cannot take an approach to partner with you to help build and grow your business!

Please do not hesitate to ask further questions. We are always open to a conversation with a new or existing client!



Tim Porter, CPA, CISA

Director

tporter@peasebell.com



Jenn Kenney, ISO 27001 CIS LA

Manager

jkenney@peasebell.com