Preparing for Your Next SOC 2 Audit

The goal of your subsequent SOC 2 audits is to build upon the foundation of your previous SOC 2 reports and continually prove to your customers that your organization prioritizes data security, privacy, and compliance. This ongoing effort demonstrates your commitment in protecting your clients' data and adapting to new challenges, while building trust, lowering risks, and keeping you up with industry standards.

Important:
Your customers will expect to see an updated report on an annual basis, and you don't want to be caught without one when they ask for a refreshed report.

Review and Maintain Your Vanta Account

With a foundational SOC 2 framework established from previous years, it's important that you consistently review and verify the accuracy and relevance of all information within your Vanta instance. Below, we will break it down into two sections to help you:

Review Recurring Controls

- **Policies**
  Policies should be updated, at least annually, to implement any necessary changes.
  - All policy approved dates should be within the last 12 months.
- **Documents**
  Documents need updated either on a quarterly or annual basis, depending on recurrence.
  - Review using our Document Guidance to update and approve all existing documents in Vanta.
  - Review all items you previously marked N/A to see if they are now relevant.
- **Vulnerabilities**
  Vulnerability scans should be conducted at least quarterly.
  - Address vulnerability findings to be sure all are up to date.
  - If you use a 3rd party scanning tool that does not integrate with Vanta, you will need to upload screenshots to the associated tests in Vanta.
- **Risk Management**
  Risk assessment should be updated annually.
  - Review and make needed updates to your risk assessment. Then, take a new snapshot in Vanta once completed.
- **Vendors**
  Vendor reviews should be conducted annually.
  - Review all vendors and add/remove any vendors you see fit.
  - Review the associated risk assigned to each vendor.
  - Update security reviews for High/Critical vendors annually, which includes uploading and reviewing their updated security report.

Ongoing Maintenance

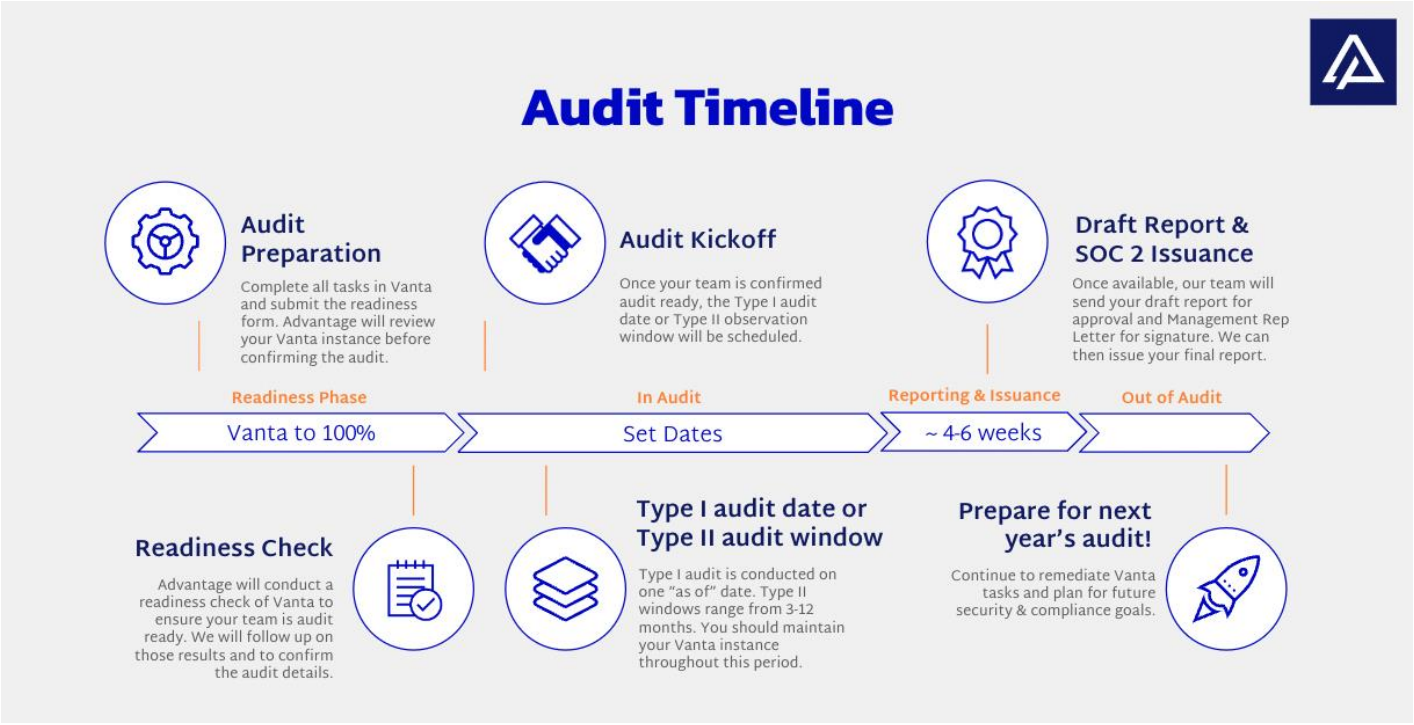
- **Tests**
  - Maintain that all tests are in a passing state.
  - Review previous tests marked N/A and assess if they are now relevant.
- **Integrations**
  - Confirm that all tools integrated with Vanta are still reflective of your infrastructure and review if additional resources need to be added to the scope of the audit.
- **Previous years findings (if applicable)**
  - Review previous years' findings and implement any remediations.

Advantage Partners Advisory

We understand that SOC 2 audits demand a lot of your time and energy. We can help! Ask us about our Advisory offerings to help manage your compliance for you.

Transitioning From Type I to Type II

To enhance your security standing, we recommend pursuing a Type II audit next if you completed a Type I in your first year. You might wonder why pursue a Type II over Type I? Well, a SOC 2 Type I is a snapshot audit, evaluating the design and implementation of controls at a specific point in time. Whereas a SOC 2 Type II audit is conducted with an observation window that typically ranges from three to twelve months, and your auditor will attest to the operating effectiveness of your controls over the entire observation period.



Because the Type II audit attests to the effectiveness of the controls over a period, your customers will feel more confident in your security posture. Here are some expectations for a Type II audit:

- Observation window (in audit) of 3-12 months
  - *If you had a three-month audit window the previous year, we recommend you consider scheduling a longer observation window this year.*
- Reporting phase is 4-6 weeks
- With the extended observation period, it would be important to consider scheduling your audit at least 3 months earlier (depending on your preferred audit window), to maintain uninterrupted SOC 2 compliance.

Recommendations for Maturing Your Security Program

Now that you're gaining confidence in the SOC 2 realm and seeking ways to enhance your security posture, we have some additional recommendations for you to consider. If you are interested in any of the below, please reach out to customers@advantage-partners.com to discuss in more detail.

- **Penetration Testing**
  - Pen tests are a security check on your vulnerabilities where a simulated attack is conducted on your computer system, network, or app to find weaknesses. The goal is to discover and fix issues before someone with mallicious intent does so themselves.
- **Longer Observation window**
  - If you conducted a 3 month audit last year, we recommend extending the audit window to 6 or 12 months for the current year to exemplify continuous compliance.
- **Enhanced Vanta Products**
  - One consideration for improving your security program is furthering the automation of your security & compliance monitoring. The Vanta products below can assist with removing manual efforts relating to certain controls. Contact the Vanta team for further information on:
    - Access Management
    - Vendor Risk Management
    - Risk Management
    - Trust Center

Scheduling Your Next Audit

SOC 2 should be viewed as an annual audit. Your report will not expire, however, it will be considered stale about a year out. Our recommendation is to aim to align your audit end dates each year. We've included some points to consider below:

⇒ If you are transitioning from a Type I to Type II, you would want to factor in at least a 3 month observation window to your audit scheduling.
⇒ Your organization can repeat your same audit details for your next SOC 2.
⇒ Or you can extend the length of your observation window and start your audit earlier.

The audit length is at your discretion but it could be influenced by specific requests from your customers or as a measure to exemplify your maturing security program. If your Vanta instance has been monitored and maintained since your last audit, your team should be ready to schedule your next audit as needed.

Use our guidance above on how to maintain your Vanta instance and this Vanta Help Article to confirm when you are ready to proceed. **Once you feel that you are audit ready, use this Audit Readiness Form to notify our team.** Upon receipt, our team will review your Vanta instance and confirm your next audit details.

We'll let you know if we see any barriers and if we feel that everyone is prepared to proceed. Our team will keep you updated at every point of your audit journey!

Contact Advantage Partners

Website: https://advantage-partners.com/
Email: customers@advantage-partners.com