Vanta

The SOC 2 Compliance Checklist

The SOC 2 Compliance Checklist

Most businesses look at security compliance as a mountain that is impossible to conquer without an equally mountainous budget and ample time with endless frustrations. The truth is that every organization's experience will vary, but in most cases, you can achieve compliance and certification easier than you think if you only prepare properly.

That begins with educating yourself about the road ahead and having the right tools in your toolbox, like automated compliance software. If you're preparing to guide your organization through SOC 2 compliance, our SOC 2 compliance checklist will break down the process and give you a digestible view of the road ahead.

STEP 1

Pre-work for your SOC 2 compliance

- [ ] **Choose the right type of SOC 2 report:**
  - → A SOC 2 Type 1 report assesses how your organization aligns with the security controls and policies outlined in SOC 2
  - → A SOC 2 Type 2 report has all the components of a Type 1 report with the addition of testing your controls over a period of time
  - → The correct report will depend on the requirements or requests of the client or partner that has requested a SOC 2 report from you
- [ ] **Determine the framework for your SOC 2 report. Of the five Trust Service Criteria in SOC 2, every organization needs to comply with the first criteria (security), but you only need to assess and document the other criteria that apply. Determining your framework involves deciding which Trust Service Criteria and controls are applicable to your business using our Trust Service Criteria Guide.**
- [ ] **Estimate the resources you expect to need. This will vary depending on how closely you already align with SOC 2 security controls, but it can include several costs such as:**
  - → Compliance software
  - → Engineers and potentially consultants
  - → Security tools, such as access control systems
  - → Administrative resources to draft security policies
  - → Auditing for your compliance certification
- [ ] **Obtain buy-in from your organization leadership to provide the resources your SOC 2 compliance will need.**

STEP 2

Work toward SOC 2 compliance

- [ ] Begin with an initial assessment of your system using automated compliance software to determine which necessary controls and practices you have already implemented and which you still need to put in place.
- [ ] Review your Vanta report to determine any controls and protocols within the “Security” Trust Service Criteria that you do not yet meet and implement these one by one. These are multi-tiered controls across several categories of security, including:
  - → CC1: Control Environment
  - → CC2: Communication and Information
  - → CC3: Risk Assessment
  - → CC4: Monitoring Activities
  - → CC5: Control Activities
  - → CC6: Logical and Physical Access Controls
  - → CC7: System Operations
  - → CC8: Change Management
  - → CC9: Risk Mitigation
- [ ] Using Vanta’s initial assessment report as a to-do list, address each of the applicable controls in the other Trust Services Criteria that you identified in your initial framework, but that you have not yet implemented.
- [ ] Using Vanta’s initial assessment report, draft security policies and protocols that adhere to the standards outlined in SOC 2. Vanta’s tool includes thorough and user-friendly templates to make this simpler and save time for your team.
- [ ] Run Vanta’s automated compliance software again to determine if you have met all the necessary criteria and controls for your SOC 2 report and to document your compliance with these controls.

STEP 3

Complete a SOC 2 report audit

- [ ] Select and hire an auditor affiliated with the American Institute of Certified Public Accountants (AICPA), the organization that developed and supports SOC 2.
- [ ] Complete a readiness assessment with this auditor to determine if you have met the minimum standards to undergo a full audit.
- [ ] If your readiness assessment indicates that there are SOC 2 controls you need to address before your audit, complete these requirements. However, if you have automated compliance software to guide your preparations and your SOC 2 compliance, this is unlikely.
- [ ] Undergo a full audit with your SOC 2 report auditor. This may involve weeks or longer of working with your auditor to provide the documentation they need. Vanta simplifies your audit, however, by compiling your compliance evidence and documentation into one platform your auditor can access directly.
- [ ] When you pass your audit, the auditor will present you with your SOC 2 report to document and verify your compliance.

STEP 4

Maintain your SOC 2 compliance annually

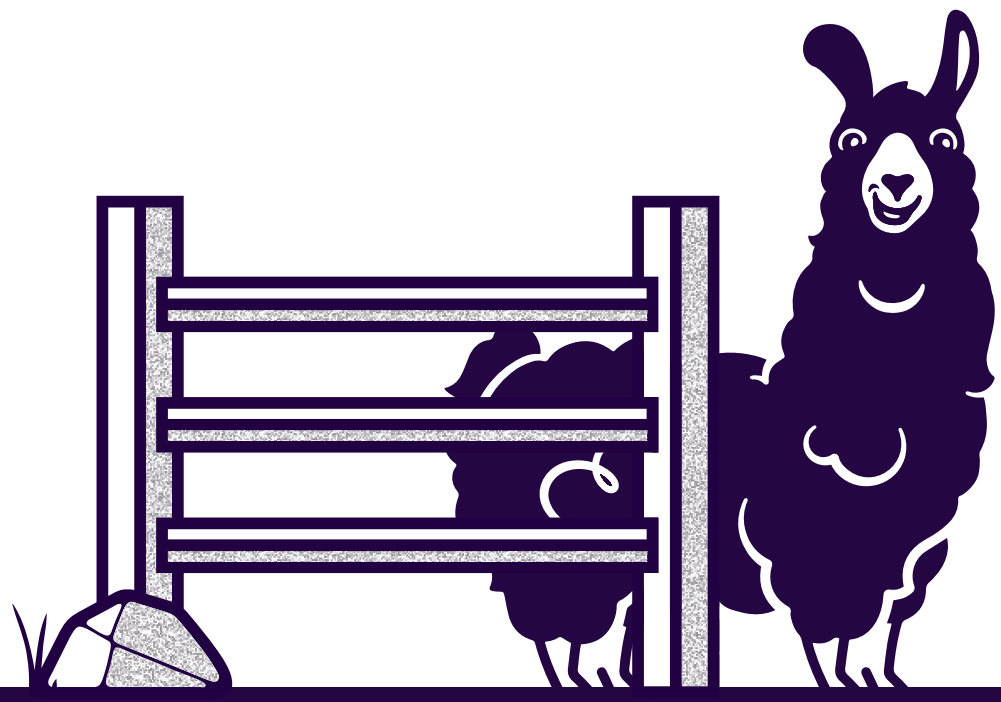
- [ ] Establish a system or protocol to regularly monitor your SOC 2 compliance and identify any breaches of your compliance, as this can happen with system updates and changes.
- [ ] Promptly address any gaps in your compliance that arise, rather than waiting until your next audit.
- [ ] Undergo a SOC 2 re-certification audit each year with your chosen SOC 2 auditor to renew your certification.

Prioritizing Your Security and Opening Doors with SOC 2 Compliance

Information security is a vital priority for any business today from an ethical standpoint and from a business standpoint. Not only could a data breach jeopardize your revenue but many of your future clients and partners may require a SOC 2 report before they consider your organization. Achieving and maintaining your SOC 2 compliance can open countless doors, and you can simplify the process with the help of the checklist above and Vanta's compliance automation software.

Request a demo today to learn more about how we can help you protect and grow your organization.

Request a demo →



Vanta

Automate compliance. Simplify security. Demonstrate trust.

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies rely on Vanta to build, maintain and demonstrate their trust—all in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

For more information, visit: **www.vanta.com** | **sales@vanta.com**