PivotPoint SECURITY

How to Effectively Use a Vendor's SOC 2 Report in Your VRM Program

In a recent blog post, we covered the many benefits of having a shorter **vendor due diligence questionnaire**, and explained how your organization can accomplish the same level of risk identification with a shorter questionnaire through various methods, such as **relying on independent third-party attestations**.

This guide will cover how to confidently increase your reliance on third-party attestations, particularly a SOC 2 Type 2. **Using the guidance to follow, you can achieve the same level of due diligence as if you had sent the vendor a lengthy questionnaire – and have even more trust in the data.**

Why the SOC 2?

We are highlighting the **SOC 2** because it **is one of the most helpful reports for understanding vendor risk.** These reports cover multiple important controls related to information security, availability, processing integrity, confidentiality and privacy. **A typical SOC 2 report will provide a higher level of assurance than a simple due diligence questionnaire**. SOC 2 compliance audits can sometimes take many months, and typically involves onsite procedures performed by an independent and reputable audit firm.

While a SOC 2 report should cover many of the control areas and questions you may have regarding a vendor's security posture, sometimes reports are not consistent as the vendor being audited can provide input on which control groups are relevant. Addressing the following questions can help ensure all of your bases are covered.

Who is the independent service auditor issuing the report?

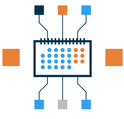
At the top of the report is the name of the organization that issued the SOC 2 report. You should be asking several questions about them:

- Are they **reputable**?
- **How long** have they been issuing these reports?
- Are they **qualified** to perform these services?
- Do they have the appropriate **certifications** or **qualifications** to issue such a report?

What is the auditor's opinion of the vendor's controls?

Is the opinion **unqualified** (good)? Or **qualified** (not perfect, but passable overall)? This means one or more controls were not designed or operating effectively relative to the objectives and were therefore deemed unreliable. This is not uncommon, and can reflect **problems with new controls**, or **with controls that operated successfully in the past but are now less effective** due to employee turnover or the implementation of new processes. Or is the opinion adverse, meaning the control framework overall is not operating effectively?

If an opinion is qualified, you need to find out why, and **determine whether the compromised control could impact your data security**. If an opinion is adverse, that's obviously not a good sign and you might want to consider shopping for a new vendor.



What time period does the report cover?

Did the vendor send a copy of their **most recent report**? If not, why has the vendor not performed **annual SOC 2 audits**? Is there a **bridge letter** available? Asking these questions will ensure you are looking at the most recent report of the vendor's environment and help uncover whether the vendor is hoping to hide **more recent and presumably less favorable findings.**

What scope of services does the report cover?

Did you receive the correct report? Many organizations have several different SOC 2 reports covering different services they offer. Be sure to read **the description of the services** covered to ensure you are reviewing **the correct report**.

Does the report list any subservice organizations?

Does the vendor utilize **subservice organizations** to provide their services? If so, which method (carve-out or inclusive) was used to document their activities for this SOC report? With **the carve-out method**, the scope of the report excludes the control activities performed by the subservice organization(s). For this method, the service organization would include the services provided by the subservice organization(s) as part of the description of their own services provided, **as if the subservice organization(s) were a part of the service organization**.

With **the inclusive method**, the scope of the report includes a list of the control activities performed by the subservice organization, clearly defining the services provided by subservice organization(s). At the end of the day, **subservice organizations can increase the risk a vendor poses to your organization,** if not properly accounted for.

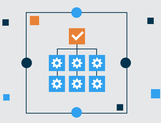
What are the controls your organization is responsible for?

Sometimes these controls are called **User Control Considerations, Complementary User Entity Controls**, or **Description of Client Considerations**. They are assumed to be in place at your organization to ensure everything works seamlessly between your organization and the vendor. You should review each listed control thoroughly to ensure no gaps exist.

What controls does the report cover?

Since the vendor is able to omit certain control areas not deemed relevant to them, **certain controls that are important to you may not be covered**. In such cases – and in general – you should view a SOC 2 report not as a comprehensive source of vendor data, but as supplementary to your **other vendor risk management activities**, such as due diligence questionnaires.

You can **customize a questionnaire to cover control areas that are important to you but not covered by the SOC 2 report**. For example, if employee background checks and training are extremely important to you, and are not covered in the report, your due diligence questionnaire and document request list can include items to ensure you understand the vendor's controls in that area. Likewise, if uptime monitoring is important to you, be sure to include this as part of your due diligence questionnaire.



What are the results of the controls testing?

Were any **exceptions** identified? If so, were **management responses** appropriate? Any exceptions noted should be thoroughly reviewed, understood, and followed up on (if appropriate).

If used well, a **SOC 2 report can help save a significant amount of time with vendor reviews**. In fact, a major reason vendors will often go through the effort and expense of completing a SOC 2 is to make their lives easier around managing their customer questionnaires as well. If you request information that is important to you, but beyond the scope of a vendor's current SOC 2, you may often find that information included in **subsequent reports**.

If you'd like additional guidance on managing your vendor risk, including how conduct simple, effective, and efficient vendor reviews, **Contact Pivot Point Security**

We have a strong focus on simplifying VRM programs for medium to large enterprises

info@pivotpointsecurity.com

PivotPoint SECURITY