SCHNEIDER DOWNS

Big Thinking. Personal Focus.

OUR THOUGHTS ON

Third Party Risk Management Insights

Secrets Revealed: What Your Third Party Auditors Don't Want You to Know

When it comes to matters of IT security assurance, there is at least one guaranteed "assurance" – that there's no one-size-fits-all approach to IT security.

Our IT Risk & Compliance and Cybersecurity teams at Schneider Downs have had the pleasure of working with many different types of security teams, part of many different types and sizes of global corporations and organizations, in varying industries. It is high time to give back to the people who enabled us to gain such world-class experience in our fields.

Nausea, Heartburn, Indigestion, Upset Stomach... IT questionnaire requests! If your organization frequently receives vendor questionnaire requests, has varying levels of customer requirements, or has experienced third party risk assessment scope creep, this article is for you. We're here to simplify your response and quiet the noise from the all too common security seesaw.

Symptoms First, let's define that term – security seesaw. This alludes to the idea that certain compliance and security practitioners have slightly different objectives. *Generally speaking*, where a compliance practitioner's main goal is to achieve compliance within an established framework, regulation, organizational requirement, etc., a security practitioner's goal is to effectively protect organizational assets from potential threats. To be very clear, our teams at SD work on both sides of the floating fence, so we empathize with both schools of thought. Fortunately, both parties do share one common goal that bring us all together: managing and mitigating risk!

Diagnosis Question: So, you have multiple customers with different requirements. Many of whom are asking the same questions in a different way. How can your organization normalize these requests to achieve higher efficiency, while still meeting, and potentially exceeding customer demands?

Answer: Work together to achieve the same goal in managing and mitigating risk. Each side of the security and compliance coin needs to understand the objectives of the other party in order to reach and achieve that common goal.

So called, "Gotcha" auditors are hopefully few and far between anymore. It's common now that your auditor has a much more relationship-driven style of auditing, intended to work with people rather than against them (if not, we could probably recommend a few!). This style stems from basic concepts of humanity and affirms the idea that you can work together through that common goal.

Treatment Here are some tips, tricks, and techniques we've learned along the way for how to effectively work with third party auditors:

1. Third party audits start and end with a contract. That contract is the holy grail of your customer relationship and is also the foundation of your control requirements. Many contracts require a third party audit, not necessarily a specific control. Best practice TPRM guidance requires organizations to ensure a commensurate level of control with each relationship. However, the specific controls you implement to mitigate risk should be negotiable (if all parties talk in terms of risk mitigation).
    a. There's more than one way to bake a cake, and there's more than one way to mitigate risk. The controls being requested by third party auditors aren't the end all, be all. Consider and discuss other options to mitigate risk to find the balance of security vs. functionality that is acceptable for both parties.
    b. Consider "accepting" the risk. Should your organization be unwilling to implement a certain control (due to cost or business rationale concerns), consider a contract amendment to accept the risk, should that risk ever be exploited.

2. As you plan for an upcoming third party risk audit/assessment, pay particular attention to the scope of the engagement. Focus closely on the data elements that your organization "processes" (stores, transmits, accesses, etc.) on behalf of your customer. The systems and controls surrounding these data elements are all that should be relevant.

   a. If you're unsure about what data elements are "processed," clarify.

3. Most standards-based assessment reports don't show the tests that are performed to determine operating effectiveness. The only standards-based assessment reports that show these tests are SOC 1 Type II and SOC 2 Type II reports. Every other type of standards-based assessment report only shows the design of the controls or the results of the tests (For example, ISO, HITRUST Certifications, PCI, SOC 1 Type I, SOC 2 Type I, SOC 3, etc.)

   a. Don't be surprised if your third party auditor can't leverage standards-based assessment reports that aren't a SOC 1 or 2 Type II.

4. Consider isolating customer data. If you're not willing to budge on certain security requirements within your frequently used environments, consider isolating the in-scope customer data that your customers are concerned with. Specifically, air-gapping is an effective network security measure to physically isolate networks and/or interfaces. However, there are many ways your organization can isolate data and limit third party requirements.

5. If you have a list of findings that you accepted, don't commit to a timeline that will cause an issue. Timelines are negotiable. The key word to remember here is, "reasonable." If everyone agrees that timelines are fair and reasonable, then you'll generally fulfill your third party requirements.

6. Customers that need certain your organization to implement specific controls without leeway might not be speaking in terms of risk. For example, customers that "need you to obtain an ISO certification" or "need you to change your passwords every 30 minutes."

   a. Consider asking what the risk they're concerned with is, and what could happen if the risk was exploited (i.e., understanding why it is a requirement) to get to the bottom of the concern.

7. Cloud requirements – that's right, third party auditors are concerned with more than just third parties, namely fourth and potentially fifth parties. If your customers are asking about your cloud vendor, it's your responsibility to uphold their third party requirements for your vendor, and you might need to do so to the same degree you're being held accountable.

   a. Fortunately, cloud service providers are facing the same third party requirements you are and can often provide a SOC 2 Type II report to independently demonstrate security assurance.

8. Concerned with your upcoming contract renewal? Or better yet, seeking a first-time contract with a new customer?

   a. Regardless of the number of egregious gaps that are found during a third party audit, you can generally still satisfy a third party auditor by documenting comprehensive remediation procedures. Ultimately, we want to see that you care about your security and have plan.

9. Are your third party auditors not accepting your SOC Report? Or asking questions above and beyond what was tested within the SOC report?

   a. If you're being asked to map your SOC controls to your customer's questionnaire or if they have questions above and beyond what was tested in the SOC report, then you're receiving valid requests. This just means that your customer has a higher sensitivity to risk. Refer to the first sentence of this article again. Security isn't a one-size-fits-all-approach, and different customers/third party auditors are going to have different requirements based on their risk appetite. Good news is there are a few easy ways to handle this sort of request:

      i. Have your SOC auditors map the control crosswalks for you. They are, after all, the ones that independently designed and tested your controls. They might have a more intimate relationship with the wording of your controls than you do.

      ii. Add the controls that your third party auditors are requesting to be tested to your future SOC report. This will further enable you to adhere to the "test once, provide to many" approach of TPRM.

10. Last but not least – we know your policies and procedures are "Top Secret." We also know that they're generally nothing we haven't seen 100 times over :)

How Can Schneider Downs Help?

Schneider Downs is a registered assessment firm with the Shared Assessments Group, the clear leader in third-party risk management guidance. Our personnel are experienced in all facets of vendor risk management, and have the credentials necessary (CTPRP, CISA, CISSP, etc.) to achieve meaningful results to help your organization effectively achieve new vendor risk management heights.

For more information, please visit www.schneiderdowns.com/tprm or contact us at contactsd@schneiderdowns.com

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

Pittsburgh
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

Columbus
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

Washington, D.C.
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003