

A Quick Guide

HOW TO MANAGE FOURTH-PARTY RISK

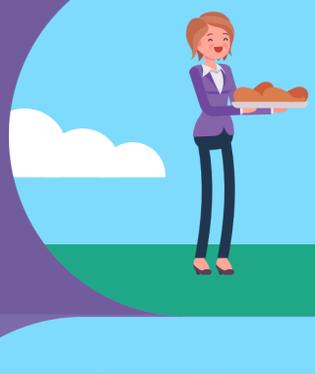


Monitoring your fourth parties is becoming an increasingly important part of vendor risk management practices. Contrary to the name, there is more to third-party risk management than just third parties.

Third Party

You have vendors you're directly contracted with – have a direct written agreement to provide your organization a product or service. They are your third-party vendor.

Example: Your Software as a Service (SaaS) provider.



Fourth Party

Your vendor may have multiple vendors of their own to assist in the delivery of the product or service you're receiving, making them your fourth-party vendor. Your third-party vendor has a direct contract with them, but you do not.

Example: Your SaaS provider's cloud vendor.



Other Parties

The relationships can go on. Fourth parties could be contracted with vendors, making them a fifth party to you, and those fifth parties could be contracted with vendors, giving you sixth parties.

Example: The cloud vendor's internet service provider.



While third-party risk management is about managing third parties, it's also incredibly important to be aware of your fourth parties, fifth parties and more... especially if your data is being passed through those connections.



Third & Fourth-Party Data Flow

When you share data with your third-party vendor, they can share it with their vendor (your fourth party) and they may continue sharing it and it continues down the line of other vendors. There may be a very long tail on where your data or customer data could end up – data that you and your organization are responsible for.

The 5 Initial Steps of Fourth Party Oversight

How can you feel confident in knowing the data is being protected? Just because your organization may have great security measures in place to protect your business and customer data, does NOT guarantee your third parties and their third parties are doing the same.

Step 1

Acknowledge criticality.

Understand the importance of conducting due diligence on a fourth-party critical vendor. Since they have access to your confidential information, fourth parties are just as important as third parties. Make sure that they understand your rules regarding the use and security of non-public information.

Step 2

Review your third party's vendor management program.

Understand what they do, how effective it is and how you can monitor it. Ensure it meets your expectations as you will have to rely on it.

Step 3

Leverage your third parties.

It can be difficult to know who the fourth parties are to monitor. This step has become a bit easier on some, thanks to the SSAE 18 requirements that went into effect in May 2017, as your third parties should now be disclosing significant subservice providers; however, it's an audit that not all organizations have or care to get. Work with your third party to request information. Since you don't have a contract with the fourth parties, you will need their assistance to get all of the information you need. As they provide you with the fourth party's due diligence, review everything thoroughly, just as you would your own third party's due diligence.

Step 4

Get it in writing.

If possible, contractually require your third party to notify you prior to doing business with a significant fourth party. Typically, a significant fourth party is one who is critical to your third party's business or will have access to your customer's data.

Step 5

Understand your relationship matrix

Often, you can leverage your existing third-party risk management software tool, as this is an easy way to capture the data and run comprehensive reports, or you can track the information separately. The things you need to know are:

- Your critical and high-risk third parties (specifically those who have your data).
- Who your fourth parties are (while you may not capture all of them, you must know any who have access to your data or are critical to your third party).
- A description of your vendors to help maintain an accurate description of the relationship between your third and fourth parties.
- The fourth parties who work with more than one of your third-party vendors, to ensure you're aware of any overlap.

What to Do If You Can't Obtain Information

- **Determine if another way to view the information will suffice.** Maybe an alternate document can be provided or your vendor can screenshare, so that you don't have a physical file, etc.
- **Request your third-party vendor write the request into their contract renewal.** Make it a contractual obligation to provide the due diligence needed.
- **Document everything you've done to obtain the information.** Keep notes about each request with a date and time stamp.
- **Notify upper management.** Keep the appropriate people informed, such as senior management, the board and/or the committee.

Monitoring a fourth party is a unique challenge and can be tricky, but responsibility of your data and your customers' information falls on you. Make every reasonable effort to protect it.

Download free sample assessments of vendor controls and see how Venminder can help you reduce your third-party risk management workload.

[DOWNLOAD NOW](#)

[PRINTABLE VERSION](#)

venminder

Copyright © 2020 by Venminder, Inc.

Manage Vendors. Mitigate Risk. Reduce Workload.

(270) 506-5140 | [venminder.com](#)