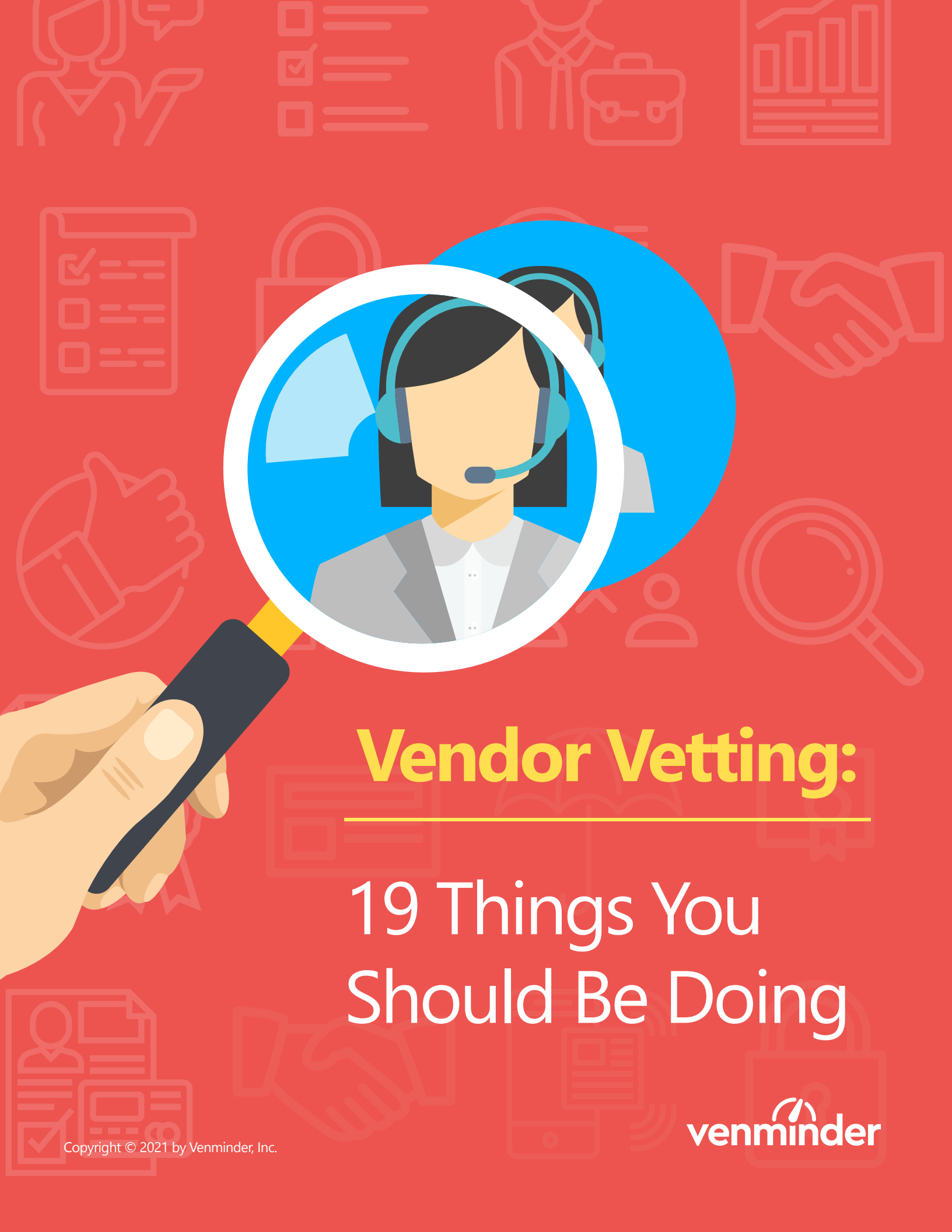


Vendor Vetting:

19 Things You Should Be Doing

venminder

Vendor Vetting:
19 Things You Should Be Doing

Chances are, your organization, like many others, has an extensive list of vendors at varying risk levels that require different types of due diligence and ongoing monitoring. However, regardless of risk level, there are 19 things you should be doing for every vendor.

It might seem obvious to review these 19 items for your critical or high-risk vendors, but what about your other vendors who pose a lower level of risk? The truth is that any of your vendors can potentially harm your reputation, risk customer relationships and put you at risk for regulatory fines. Proper due diligence early on could help prevent these situations altogether.

Bottom line? Don't overlook these 19 items on any vendor/organization with which you do business.

1 Negotiate

What?
Come to an agreement on the contract terms and provisions.

Why?
It's important to define responsibilities, expectations, terms & conditions, data handling requirements and set the ground rules in conjunction with your vendor risk management policy.

How?
Have your designated contracts team work directly with the vendor contact.

2 Confidentiality Agreement

What?
An executed confidentiality agreement, non-disclosure agreement or privacy statement between your organization and the vendor.

Why?
To protect each party's trade secrets and any other confidential information.

How?
Begin with your organization's standard template and restructure as needed to accommodate requests.

3 General Information

What?
This includes basic information like the legal name and doing business as (d/b/a) or professionally known as (p/k/a), business address, physical locations, website information, etc.

Why?
This basic information should be kept on file and updated, as needed.

How?
You can find most of this information through an online search, or simply asking your vendor.

4 Secretary of State Check

What?
Confirmation the third party is properly registered in the state.

Why?
Validates the authenticity of the business.

How?
Search for the official Secretary of State website for the state in which your vendor is filed. Through this site, you'll be able to get directions for finding the right certificates.

5 Complaint Research

What?
Learn about the type and/or volume of customer complaints filed against your vendor.

Why?
Your reputation is at risk if you choose a vendor who is developing a trend towards unfair, deceptive, or abusive acts or practices (UDAAP) violations or consistently overpromises and underdelivers.

How?
There are websites that will gather complaints and report. We like these:

Bbb.org

Consumerfinance.gov

Ripoffreport.com

6 OFAC Check

What?
A check to determine if the company is owned and/or managed by any sanctioned person or nation.

Why?
This is required in order to follow U.S. Treasury laws and the anti-money laundering statute.

How?
You likely have an OFAC provider now for your customer OFAC checks, but there are also sites that provide quick one-off checks. Try this:

Treasury.gov

7 Articles of Incorporation/ Business License

What?
Proof of a specific business license is required (when applicable – i.e., money transfer license) and proof the business entity is properly organized.

Why?
This fundamental item ensures that you "know your vendor" by confirming that they're properly licensed to provide the product/service for which you're contracting.

How?
Request these documents directly from the vendor.

8 State of Incorporation

What?
Confirmation the entity is incorporated, is filing tax returns and is a legitimate business.

Why?
You want to make sure you're dealing with a real company that is registered with the state in which it was incorporated.

How?
Refer to the Secretary of State website for the state in which your vendor is incorporated. This site will allow you to search for incorporated entities.

9 Tax ID

What?
IRS tax identifier and any state tax identifiers.

Why?
Ensures that they're appropriately registered with the IRS, with the state of incorporation and the state in which they intend to do business.

How?
Request this directly from the vendor.

10 Dun & Bradstreet (D&B) Report

What?
Business credit and trade report.

Why?
This report may convey incremental details on a vendor's financial and credit profile not found within a set of audited or company-prepared financials. It can also speak directly to the reputation of the vendor when it comes to payment habits.

How?
You can obtain this directly from D&B or other aggregate providers.

11 Negative News Search

What?
This will reveal any reports that are potentially damaging to your vendor's reputation.

Why?
It's a good idea to avoid surprises. A vendor is unlikely to offer any news that puts them in a negative light. This is a simple but effective way to ensure you go into every new vendor relationship with your eyes wide open.

How?
Do a Google News search for the vendor's name:

Google.com/news

12 Credit Report

What?
A credit check on the vendor.

Why?
A poor credit report could identify underlying issues such as a decline in financial condition or failing business operations.

How?
Perform an online search. Try these:

Equifax.com

Transunion.com

Experian.com

13 Ownership Structure and Affiliated Companies

What?
An organization structure and an organization chart will provide details on the corporate ownership.

Why?
You need to know the overall corporate structure, so you know the real strengths and weaknesses of the company. It also gives you insight into potential operational issues.

How?
The vendor you're vetting should provide this to you as part of the due diligence packet.

14 Certificate of Good Standing

What?
Local Better Business Bureaus (BBBs) and state treasurers will have two different types of certificates that show good standing.

Why?
The state may issue one to let everyone know the company is current on its tax obligation. The BBBs will also issue certificates to businesses that operate ethically and don't have too many complaints.

How?
Check out the website for the Secretary of State in which the vendor is incorporated or the local BBB.

15 Financials

What?
This can refer to audited or unaudited financial statements, which vary in their length and completeness.

Why?
Understanding the vendor's financial health is important and more than just reviewing the numbers. If their financials are declining year-over-year then there could be underlying concerns that you'll want to become aware of such as pending litigation or service level issues.

How?
If they're a public vendor, you can access the financial statement on the vendor's website. If they're a private vendor, you need to reach out to the vendor directly with the request.

16 Insurance Documentation

What?
You'll need to obtain at least two documents — a certificate of liability insurance and a certificate of workers' compensation. Cybersecurity insurance should also be required for any vendor that can access PII or that connects to your organization's network.

Why?
The liability insurance covers the employees of the company you wish to do business with and will let you know the company can financially cover an error or omission. Also, the company's employees may be injured while working for your organization, in which case the workers' compensation insurance will cover that exposure.

How?
Request the documentation by reaching out to the vendor's insurance provider. This should come directly from the insurance company(s) and not the vendor you're attempting to contract with.

17 Business Resumption and Contingency Plans *(if required)*

What?
This refers to business continuity (BC) plans and disaster recovery (DR) plans that are both updated and tested.

Why?
BC plans outline the vendor's strategies to maintain operations should an unexpected event disrupt business operations. DR plans outline how they plan to recover and how long it will take them to do so.

How?
Request these directly from the vendor.

18 Audit Documentation *(if required)*

What?
SOC 1, SOC 2 or any other information technology related audit documentation.

Why?
These audit reports will assist with reviewing the vendor's IT controls to verify they're adequate and functioning properly.

How?
Request the reports directly from the vendor.

19 List of Subcontractors/ Fourth Parties *(if applicable)*

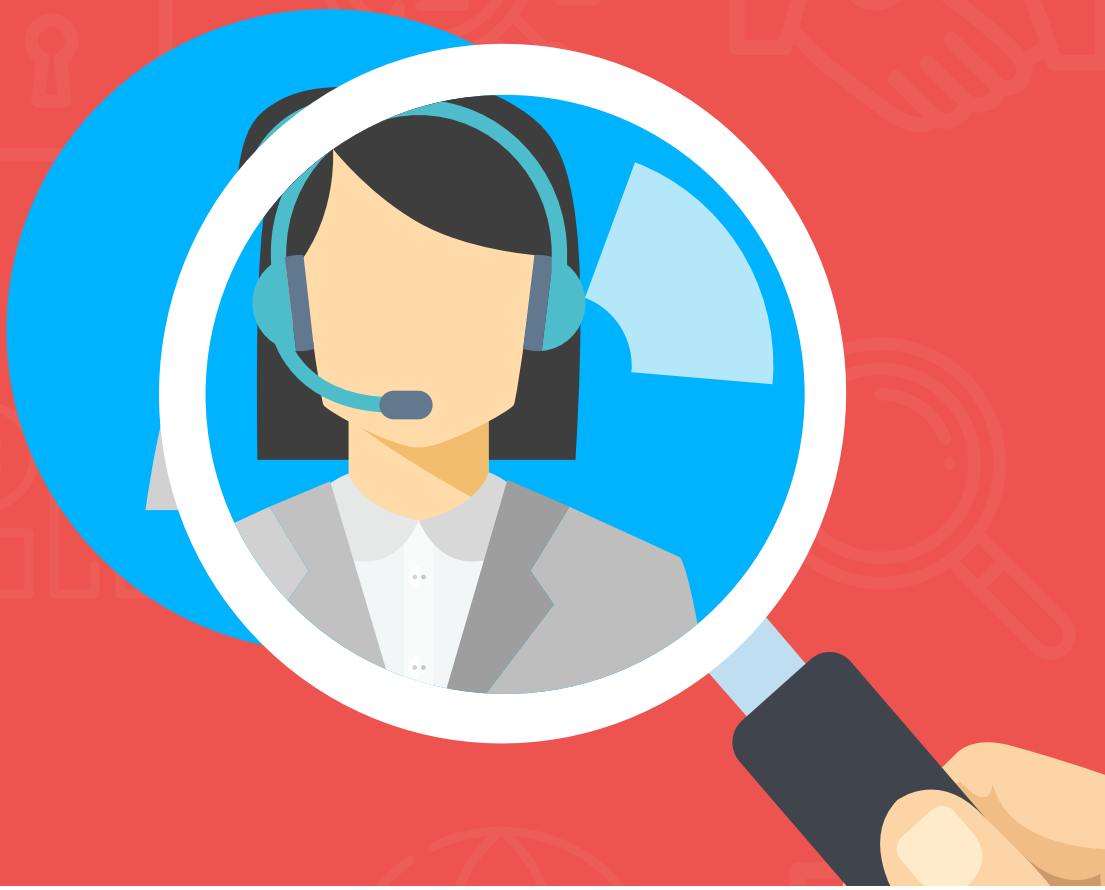
What?
These are your vendor's vendors, who don't have direct contact with your organization. However, they may have access to your data, so you'll need to know what (specifically) they've been contracted to do.

Why?
You're required to know who has what data of your organization and of your customers and what use they plan for the data.

How?
Obtain this list during the due diligence stage of your vendor selection process and make sure they're clearly stated in your vendor contract.

Download a sample initial vetting package of a third party and see how Venminder can help reduce your third-party risk management workload.

Download Now



venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance and more.