
# Vendor Reputation Risk and Its Impact



venminder

## Reputation risk occurs when negative publicity regarding your organization's business practices is reported on, often leading to declining customer trust.

Your organization's reputation and customer trust are normally impacted by a perceived or real data breach or inability to conduct business to customer expectations.

Managing your organization's reputation risk isn't just about what you're doing to protect it. It comes with an additional layer – **your organization is responsible for risks** associated with the activities of your third-party service providers, too.

If a third party is breached and it impacts your operations, no one will be thinking about your vendor's name... **It's YOUR organization's name that will be remembered.** You can have a sterling reputation based on years of established history, only to have it get annihilated by a single third-party incident.

# Reputation Risk Is Growing

There are several factors that have led to an increased risk of reputational damage.

Some of these include:

- **Growing use and reach of social media** – There's ease of access to social platforms to share reviews and complaints about a negative experience with an organization... with thousands able to view each review or complaint.
- **Nationalist geopolitics** – A country's political views and interests can have an impact on one's opinion of an organization if it doesn't align with their views.
- **Investor and consumer activism** – Activism movements to essentially force organizations to be structured one way or act a certain way that benefits investor or consumer interests can cause a lot of publicity.
- **Vulnerabilities rising from global crisis** – The COVID-19 pandemic is a prime example of how a global crisis can wreak havoc on an organization and lead to operational delays and inefficiencies, potentially leading to dissatisfied customers and reputational risk.

venminder

# 5 Reputation Risk Areas to Consider When Reviewing Vendors

Much of the information you request when performing vendor due diligence should shed some light on how likely a vendor may impact your reputation. Here are 5 areas to consider:

1. **Financial Performance.** Financial history is one of the most important pieces of information needed when evaluating the risk factors associated with a vendor, which is why requesting financial documents is such a crucial part of performing thorough due diligence. Declining financials may indicate a vendor's operations are struggling which can lead to a host of issues like declining service levels or products being discontinued… all of which could impact your own organization and its reputation.

2. **Product/Service Quality Standards.** Ensure your vendors consistently adhere to quality standards. Do they report product/service defects? Both recalls or gaps in service can severely impact your own operations and reputation.

3. **Ethics and Integrity.** It should be evident that your vendors are committed to meeting ethical standards. Take note of interactions or scenarios that are dishonest or appear fraudulent.

4. **Safety/Security.** What policies, procedures and programs does a vendor have in place? What are their training and testing protocols? A strong, proven infrastructure is crucial for protecting against cybersecurity threats and security breaches – notorious reputation killers.

5. **Crisis Response.** Vendors should have well-developed processes in place for crisis response. Think about how your vendors reacted to COVID-19. Who had a better response plan than others and what did that entail? If a vendor reacts poorly to smaller stressors or concerns, the chances are they may not be the greatest partner in times of crisis. Make your sure vendor has a formal business continuity plan and disaster recovery plan.

# **Statistics:**
# The Impact of Reputation

There's a lot on the line when it comes to your reputation. Today, consumers are inundated with countless news sources, and word of a significant event spreads with only the click of a button.

## These statistics show the impact of reputation:

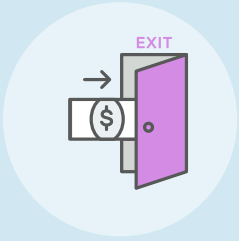
**More than**
**25%**
of an organization's market value is attributable to reputation
***– The World Economic Forum***


---

**80%**
of consumers will defect from a business if their information is compromised in a breach
***– IDC***

---

**36%**
of the cost of a data breach comes from the loss of business stemming from loss of customer trust
***– Ponemon Institute***



# Who Poses Reputation Vendor Risk?

Which of your vendors actually pose a reputational risk to your organization? All of them! So, as you're reviewing due diligence, you should determine the amount of reputational risk each one of your vendors poses to help prevent an impact on your organization's reputation.

# Determining Inherent Reputation Risk

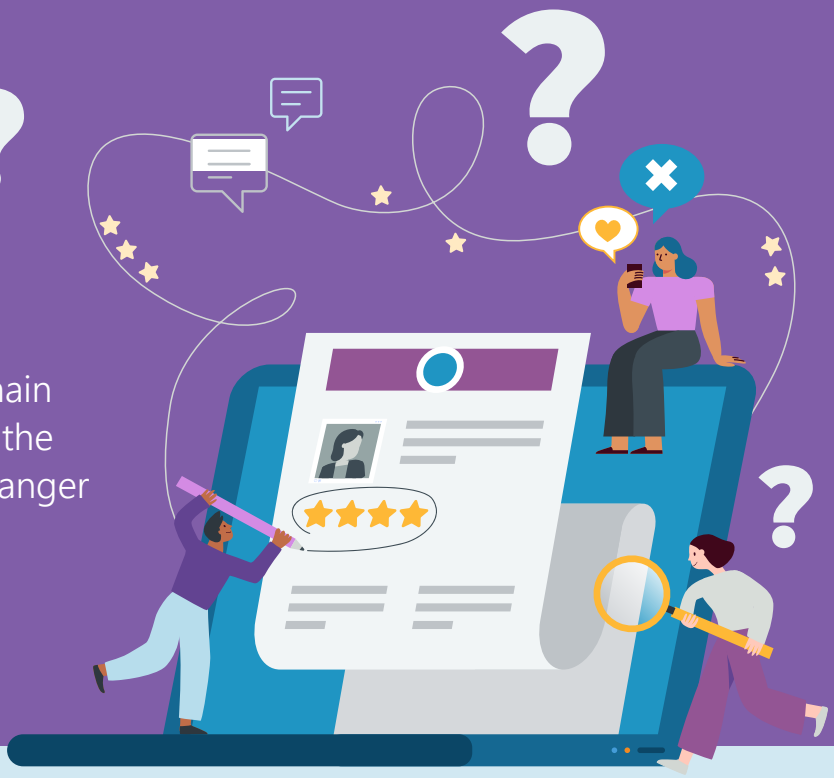
You'll want to ask questions to clearly determine the inherent risk a vendor may **directly** pose your organization.

**Some of these questions may include:**

- Does your vendor **interact** with your customers?
- Does your vendor impact **customer service**?
- Does the product/service make up a **significant percentage** of revenue?
- Do the products/services being provided require the vendor to be **in compliance** with any regulatory guidance?

This will help you better understand just how much the vendor can impact your overall reputation should something go awry.

# Questions to Help Determine Reputation Risk



There are an additional three main questions which will determine the extent in which a vendor is in danger of imposing reputation risk:

1. **Does the vendor's reputation exceed true character?** Reputation is a matter of perception. Reputation is distinct from the actual character or behavior of an organization and may be better or worse. When a reputation is more positive than its underlying reality, this gap poses a substantial risk. The opposite can also be true. Ask yourself: what is a truly a vendor's reputation in each area (product quality, financial performance and so on)?

2. **How much do the vendor's external beliefs and expectations change?** When expectations are shifting and an organization stays the same, the reputation-reality gap widens, and risks increase. For example, baselines and averages shift. An industry standard from last year may look quite a bit different this year. Pay attention to quality standards, metrics and SLAs.

   **Pro Tip:** Measure and review vendor performance from both a contractual scope AND an industry scope. Ask yourself if they're remaining competitive enough.

3. **What is the vendor's quality of internal coordination?** A major source of reputation risk is poor coordination of the decisions made by different business units and functions. If one group creates expectations that another group fails to meet, an organization's reputation can suffer. Alignment is key.

# 5 Tips to Mitigate and Manage Reputation Vendor Risk

Use the following tips to ensure you're being proactive in managing and mitigating reputation risk:

1. **Be proactive.** Don't wait for a negative event to occur before taking action. Always consider how a vendor's actions can affect your overall reputation. Don't forget to consider both third and fourth parties, and when in doubt, remember these two planning standbys: anticipate threats and analyze trends.

2. **Ask the right questions.** Ensure you have proper due diligence in place and are asking questions. This will give you basic knowledge of which vendors provide what types of products/services to your organization, are critical and high risk as well as who poses the most reputation risk.

3. **Monitor consistently.** Develop robust systems for ongoing monitoring. Set up alerts so that you receive negative news monitoring notifications. This can be as simple as a Google News alert. You may also want to make a habit of searching internet dialogues (e.g., blogs, forums, social media) to stay on top of vendor trends. Early warnings and triggers can help improve response time and avoid any last-minute surprises.

4. **Plan and establish a response strategy.** You need to be prepared should something happen to one of your critical vendors and they are in the news. Chances are your customers will come to you with questions. With a well-formed strategy, response time should be in minutes, not hours. This means your response team and point people are trained on the protocols and know exactly what to do should an event arise that could impact operations and reputation.

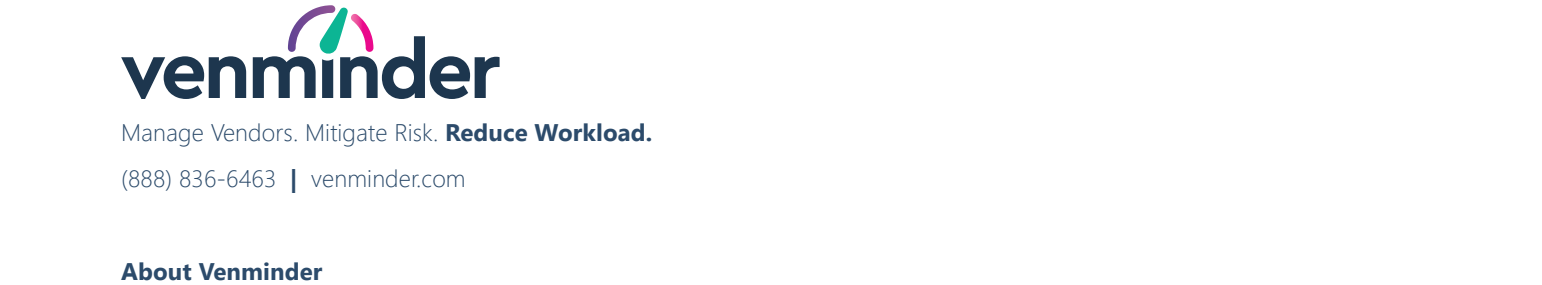
5. **Document your ongoing monitoring and assessment.** Thorough analysis is always important in third-party risk management as a whole. Be sure to document the ongoing monitoring that you plan to conduct in order to help prevent an impact on your organization's reputational risk.

**Reputation risk is every bit as important as other categories of risk, but this kind of risk can be much harder to gauge.**

To help combat the risk as much as possible, your secret weapon will be a cocktail of rigorous planning and monitoring while also consistently revisiting procedures and protocols.

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

**Download Now**



venminder

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

(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 library. The assessments enable clients 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..