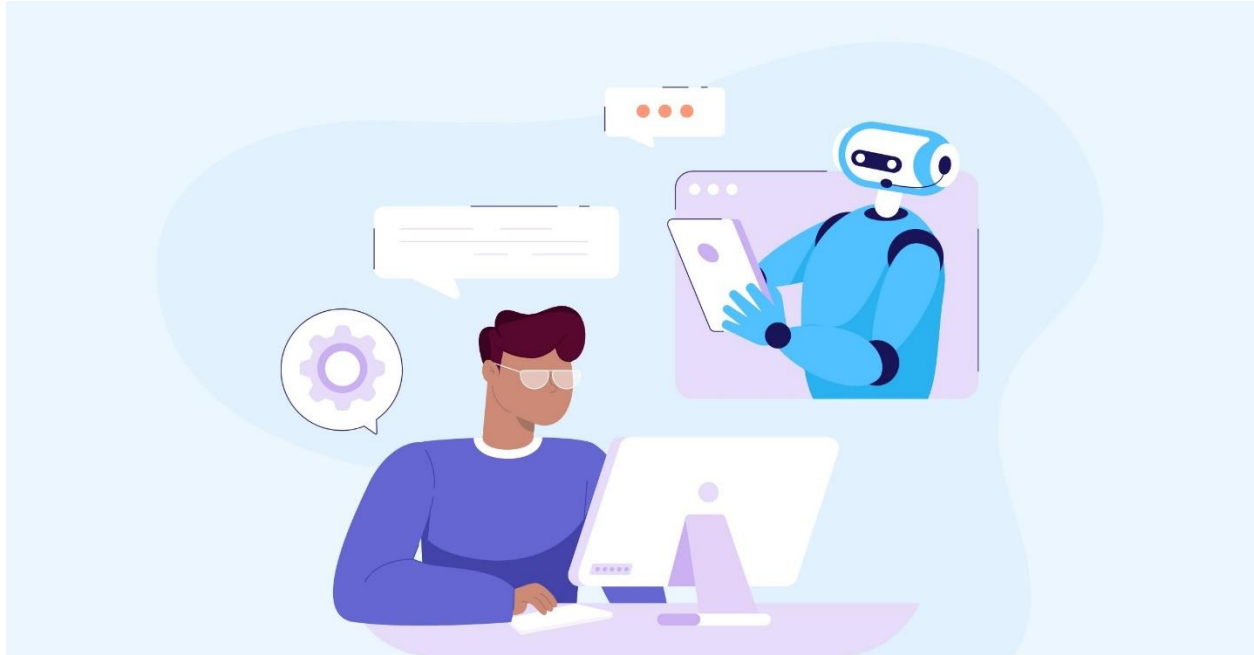


Mitigating AI Vendor Risk With Questionnaires

By: [Christine Kitamura](#) on August 15 2023

5 min read



The use of artificial intelligence (AI) has exploded within a few short years, with no signs of slowing down. Just a couple of months after its initial release, ChatGPT made history as it registered over 100 million active users. AI has seemingly impacted nearly every industry, from healthcare to manufacturing, but it's not always viewed in a positive light. The controversy around AI has even affected the entertainment industry, where it played a large role in the SAG-AFTRA strike.

Although [AI is increasingly prevalent in many organizations](#), there are still uncertainties with its risks. It's important to consider the potential impact of AI on cybersecurity, privacy, and data accuracy risks, even if your organization doesn't use AI directly. Your third-party vendors need to be evaluated for their current or planned use of AI. Maybe you've been asked to [perform due diligence](#) on an AI vendor, or maybe you're trying to determine if any of your existing vendors use AI.

With such new technology, developing a comprehensive strategy for identifying and evaluating AI risks in your [third-party risk management \(TPRM\) program](#) is essential. Let's dive into some tips that can help you get started.

Identifying AI Risk with Vendor Risk Questionnaires

You can't manage third-party vendor AI risks without first identifying where it exists in your vendor relationships. Your vendor might use AI for all or some of its processes. It may also be a crucial component of your vendor's product or service offerings.

Either way, it's important to understand how this technology affects the final product or service and consequently your organization. The [vendor risk questionnaire](#) is a document completed by the vendor. It's designed to get information on their risk practices and controls. It should be tailored to the vendor's product or service and concentrate on the risks identified in the inherent risk assessment.

Here are some sample questions you should consider asking in your vendor risk questionnaires:

- **Is AI technology used as a component of or in the research, development, or production of any of your products or services?** Different types of AI can present different levels of risk. For example, a vendor might use image recognition for research purposes, or they may use generative AI to develop a system that would interact directly with your customers.
- **Do you have plans to implement AI in any of your products, services, or operations?** Even if your vendor isn't currently using AI, they may have plans to implement it in the future, which can impact your organization.
- **Will you use AI to handle or store any sensitive data?** If your vendor has access to your organizational or customers' data, it's essential to understand whether AI will be used in its collection, processing, storage, or handling.
- **What are your processes for identifying, managing, and mitigating AI risk?** When it comes to AI risk, it's crucial to assess whether your vendor has proper measures in place to address it. This way, you can prioritize due diligence accordingly and monitor your vendor's efforts.
- **What policies do you have on employee use of AI?** Make sure you understand whether your vendor prohibits or restricts its employees from using AI for any job-related tasks. Generative AI systems like ChatGPT are increasingly common to use for job functions. It's essential to know how your vendor is managing its use among its employees.
- **Do you require employee training on the use of AI?** Although many AI systems are created to be user-friendly, there are still opportunities for this technology to be misused. Ensuring that employees understand and adhere to appropriate use is

crucial.



3 Tips for AI-Focused Due Diligence

Bringing focus to AI risk in your [due diligence process](#) might seem like a huge burden when you already have several other risk types to assess. There are a few tips that can make it an easier task:

1. **Identify associated risks.** AI brings a host of other types of risk, such as information security, business continuity, and compliance. For example, a vendor that uses an AI tool for data storage might expose you to unique cybersecurity risks that should be further evaluated. By understanding how these risk types are associated with each other, you should better understand the effectiveness of the vendor's controls.
2. **Collect relevant documents.** Depending on the information you learn through the questionnaire, you may need to request specific documents like privacy policies, employee compliance training, or licenses related to the vendor's use of AI.
3. **Collaborate with qualified subject matter experts.** Because AI risk is such a new and complex topic, it's essential to work with a subject matter expert (SME) that can provide a qualified opinion. You may need to work with different departments, like legal or information security, to ensure you have a comprehensive review of the vendor's AI risk and controls.

Third-Party AI Risk and Ongoing Monitoring

Monitoring your vendor's risk and performance throughout the relationship is always necessary, regardless of AI usage. However, AI is a rapidly changing technology that can expose your organization to unique risks, so you may decide to implement a more frequent monitoring schedule or develop a different set of standards for issue remediation.

To make the most of your [ongoing monitoring](#) efforts, remember these best practices:

- **Document new and emerging risks.** Any changes in a vendor's risk or performance should be formally documented for further review. This can validate whether the vendor is continuing to provide enough value to outweigh the risk.
- **Formalize an [issue management](#) policy.** Ongoing monitoring activities can often identify vendor issues, some of which may need immediate resolution. It's important to already have a process in place to identify, document, remediate, and close any vendor issues.
- **Check in regularly with the vendor owner.** Solicit feedback from the vendor owner by creating a framework that tracks ongoing concerns and communication. Consider meeting on a regular basis to discuss the vendor's performance and other relevant issues.

For many organizations unfamiliar with AI risks, the thought of incorporating it into your third-party risk management program can seem intimidating. However, an effective TPRM program should already have the processes in place to address some of these challenges.

As artificial intelligence increasingly impacts the business world, it's important for organizations to evaluate how their TPRM program can effectively address these emerging risks.