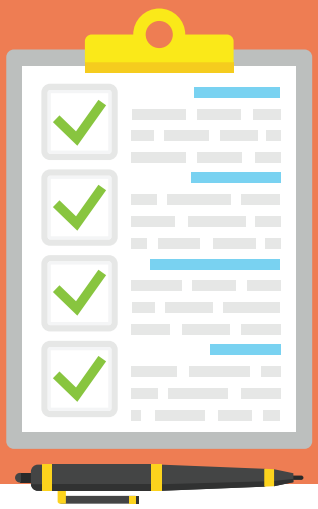
How-to Guide:

Creating a Vendor Risk Questionnaire

venminder

How-to Guide:

Creating a Vendor Risk Questionnaire



Understanding the risk, whether for new or existing third-party products or services, often starts with a questionnaire. A questionnaire shouldn't be confused with a vendor risk assessment, as they're two separate and distinct items. The questionnaire is first created and distributed to your vendors to gather the information you need. Once this is completed, don't make the mistake of filing away the answers without analyzing them. Use the results of the questionnaire in the risk assessment process to determine whether a vendor is a good fit for your organization.

Frankly, creating a questionnaire in and of itself can be quite a large task. Luckily, you have options as well as regulatory guidance to act as a guide along the way. And, you can start with either an industry standard questionnaire, such as the SIG or SIG Lite, or create your own to fit your individual needs.

How to Create a Vendor Risk Questionnaire

While some guidance is more prescriptive than others, it doesn't provide any standard templates to use for a questionnaire; therefore, it's up to your organization to determine the format that works best for you. Let's walk through the steps we recommend taking in the process:

1

STEP 1:

Consider the regulatory expectations.

For more information on what factors you should consider, the FDIC and OCC have a couple of resources — FDIC FIL 44-2008 and OCC Bulletin 2013-29 — that outline categories of risk that must be addressed depending on the product or service outsourced. The regulations vary industry to industry, and even if you're not in a regulated industry, it's a best practice to review the most stringent regulations when developing vendor risk questionnaires.

STEP 2:

Develop a rating system.

It's a best practice and regulatory expectation. This rating system is used to effectively score and report on the various categories of risk based on the information you receive from your vendor. It's recommended to always determine the criticality, inherent risk and residual risk. Criticality measures the impact on your organization that can result from the loss or disruption of the vendor's products or services. Inherent risk often determines if the risk is low, moderate or high. Residual risk is what remains after information and controls are applied to the inherent risk. What you call these ratings and the number of risk levels can vary by organization and are dependent on what is written in your policy and program documents. Don't forget that you'll have both a critical AND inherent risk level. Also, be certain that the questions are weighted appropriately – it's always a good idea to calibrate the rating using an obvious high-risk and an obvious low-risk vendor.

STEP 3:

Determine the questions to include.

You'll want to consult with your team of subject matter experts (SMEs) to develop the questions that'll be included in the vendor risk assessment(s). Include questions related to criticality and categories of risk.

The following are recommended questions to determine the ***criticality:***

1. Would a sudden loss of this third party cause a disruption to our organization?
2. Would such loss have an impact on the organization's customers?
3. If the vendor service is disrupted, would there be a negative impact on our operations if the time to restore service took more than 24 hours?

If you answer **YES** to any of these questions, then you should consider the vendor to be critical.

As each organization must define what is critical, there may be additional criteria. **Here are some examples:**

1. Are significant financial investments, resources and time required to implement the third-party relationship and manage the risk?
2. Would there be a material impact to the organization's operations or resources to engage an alternate third party or if the outsourced activity has to be brought in-house?
3. Could the third-party vendor failure negatively impact your reputation and brand?
4. Could the third-party vendor failure attract regulatory scrutiny or result in enforcement actions, including fines?

Now that you have questions to determine if the vendor is critical or non-critical to the organization, it's important to consider the inherent risk.

To determine ***inherent risk***, you'll review several categories. The risk categories will vary based on the products or services being provided. ***Some of the most common categories and associated questions include:***

1

Strategic Risk

Strategic risk occurs when a prospective or current third-party vendor's decisions and actions are incompatible with your organization's strategic objectives.

Examples of Questions to Consider:

a. Are the vendor's products or services consistent with the organization's existing services?
b. Are the vendor's products or services newly launched or an emerging technology product?

2

Reputation Risk

Reputation risk encompasses any of the numerous ways your third-party vendor could directly or indirectly damage your reputation, brand or company name. This harm could result from their actions, poor service, lawsuits, outages, fraud or data breaches.

Examples of Questions to Consider:

a. Does the vendor have direct access to your customers?
b. What is the vendor's complaint volume?

3

Operational Risk

There are two components – internal and external. Internal operational risk is broadly defined as the risk of loss resulting from a third-party vendor's ineffective or failed internal processes, people, controls or systems. Internal operational risk is specific to how things are accomplished within an organization vs. risks inherent within a particular industry. External operational risk occurs when an outside event affects your third-party vendor's ability to conduct business and impacts your organization as a result (e.g., severe weather events, fires, utility outages).

Examples of Questions to Consider:

a. Is sensitive data, such as non-public information (NPI) or personally identifiable information (PII), being exchanged?
b. Was a satisfactory OFAC check completed?

4

Financial and Credit Risk

Financial and credit risk directly relates to the financial condition of the third party itself and are important especially if the vendor has insufficient investor funding, cash or credit available to meet their contractual obligations.

Examples of Questions to Consider:

a. Has the vendor ever filed for bankruptcy?

b. Can you adequately assess the vendor's financial condition?

5

Compliance Risk

Arises from a third-party vendor's failure to comply with laws and regulations governing the products and services your organization provides to its customers. It can also be present when a vendor doesn't follow your internal policies, procedures, business standards or conduct codes.

Examples of Questions to Consider:

a. Do the products/services being provided require the vendor to be in compliance with any regulatory guidelines?

b. Has the vendor been subject to an enforcement action?

6

Information Security Risk (Inclusive of Cyber and Physical Security Risks)

Information security risk stems from third-party vendor security vulnerabilities. Two of the most common cyber risks resulting from missing or ineffective controls are cyberattacks and data breaches.

Examples of Questions to Consider:

a. Will this vendor's service require integration into your network?

b. Does this vendor's third parties (your fourth parties) have access to your sensitive data?

**The above does not represent a list of all categories or questions to be included. The examples are provided as a snippet of what's recommended to be included and doesn't comprise a full questionnaire.*

SIG vs SIG Lite Questionnaires

The **SIG questionnaire** is a holistic tool provided for risk management assessments of 18 different areas of risk such as cybersecurity, IT, privacy and data security (e.g., completed on critical business systems or high-risk vendors).

The **SIG Lite version** of the questionnaire is a shorter version of the SIG. Typically, it's used as a starting point to conduct an initial assessment of all service providers or on lower-risk vendors (e.g., hosting websites, non-critical business systems).

According to sharedassessments.org, the SIG assessments can be used in the following ways:

- By your organization to evaluate your vendor's risk controls
- Completed by your vendor and used proactively as part of a Request for Proposal (RFP) response
- Completed by your vendor and sent to their clients (aka you) in lieu of completing one or multiple proprietary questionnaires
- By your organization for self-assessment

Questionnaires By Product or Service

You should be tailoring questionnaires to the type of vendor it is – one size does not fit all. After all, do you really want to ask the landscaping company about their SOC report? Nothing will drive your vendors crazier than having a form where the questions seem like you don't understand their business and it feels like you're just going through the motions.

There'll certainly be times you need to ask follow-up questions or request additional information – think of a marketing firm or a call center, as quick examples. Once you have a good idea of how they handle disclosure changes or scripting, you'll likely want to dig deeper to get actual examples or see their compliance policies. So, you'll also need to tailor your vendor risk questionnaires and follow-ups to the vendor as deemed appropriate. Therefore, you can't expect the initial questionnaire to cover absolutely everything.

In the Venminder software, as a best practice standard **we have created four levels of questionnaires, ranging from 29 questions up to about 100 recommended questions** to include, with room to customize as much as you'd like.

In addition, **the Venminder software integrates with Shared Assessments SIG Questionnaires** to help you gather critical information to determine the vendor's security posture.

And, while the questionnaire does need to be tailored to the vendor, at the same time, with all the different types of products, services or organizations you may be utilizing, you could likely come up with an endless array of questionnaires. Stray away from doing that as it'll be very confusing and nearly impossible to manage. A better strategy would be to categorize your questionnaires.

Group assessments into a few categories:

1. A tailored assessment for your most important or critical vendors, such as your core processor
2. A more general assessment for service providers
3. Customized assessments where you know you have specific concerns, such as access to non-public information
4. Assessments tailored to specific categories (e.g., marketing, telecommunications)

As you receive answers back from questionnaires, ensure you're not getting simply "Yes", "No" or, worse yet, "it depends" to certain key questions that require elaboration. It doesn't give enough information in most cases.

Can a Vendor Risk Questionnaire Go Overboard?

A vendor risk questionnaire is certainly a necessary component of evaluating risk, but is it possible that a questionnaire can go overboard? The short answer is yes.

Here are 4 reasons why a risk questionnaire can go overboard:

- You haven't properly researched the vendor, or the products and services being provided, and you're using the wrong questionnaire to evaluate the risk level (i.e., there are too many questions that don't pertain to this type of vendor relationship)
- Your vendor risk questionnaire is too detailed or inconsistent with the risk or service presented by the vendor
- Your vendor risk questionnaire reaches a conclusion that is clearly wrong based on the vendor (i.e., your landlord coming out as high risk when you know that doesn't make sense)
- Your vendor risk questionnaire is so comprehensive that business owners don't understand it or won't help to complete it

What's Next?

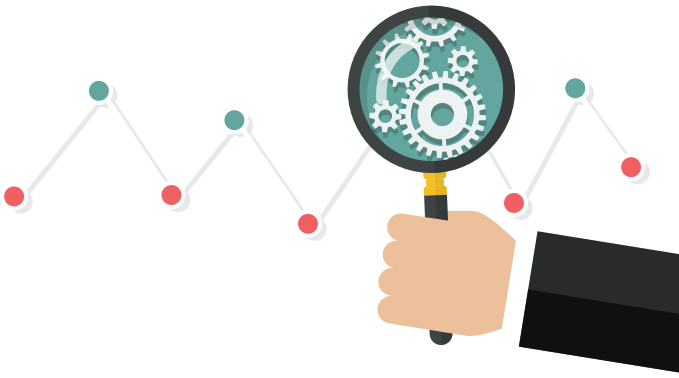
Now that you've collected the information needed through a vendor risk questionnaire, you must review and analyze the answers. Sometimes this will mean that you have to go back and forth with the vendor to understand why they responded the way they did.

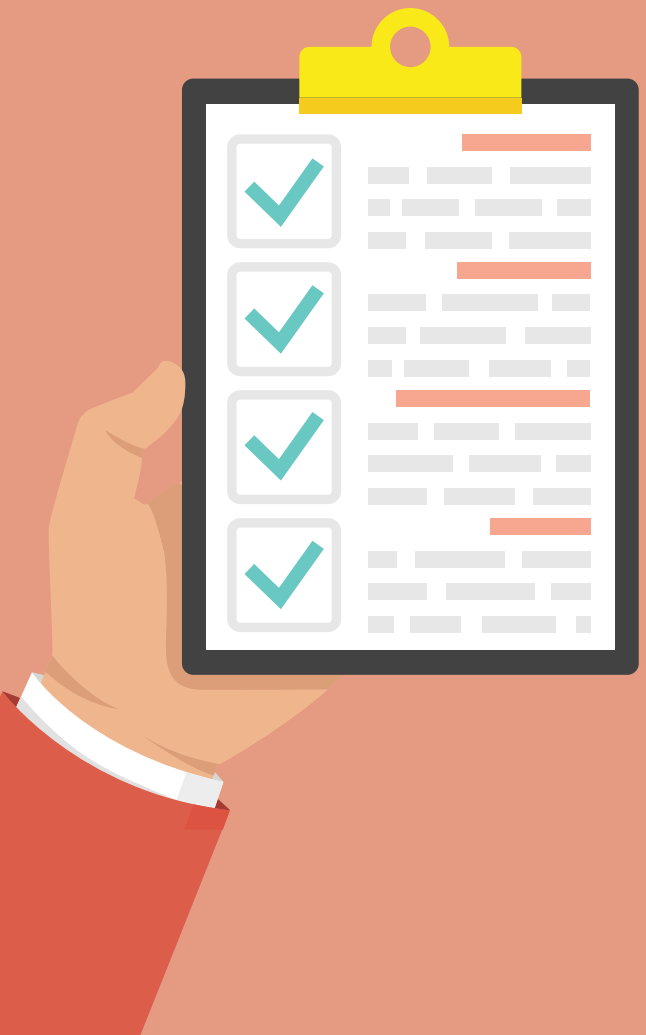
Remember, your review doesn't end there. Collecting the information is only one part of efficient third-party risk management. Next, you'll need to use this information to perform a vendor risk assessment. This step enables you to mitigate the inherent risk by implementing controls which leaves you with residual risk. Your organization must then decide if the residual risk requires any further action. So, as you can see, creating a vendor risk questionnaire is just one step in the process and there's still more to be done.

Creating and completing a vendor risk questionnaire can be a very cumbersome task that may take several iterations, but it's a vendor due diligence step that shouldn't be taken lightly. Vendor risk questionnaires lead you on the path to proper oversight. Keep in mind, risk questionnaires may be completed by the vendor in conjunction with your organization but, ultimately, the responsibility for identifying and mitigating risk belongs to your organization. The vendor risk questionnaire is your go-to resource to initiate your vendor risk assessment process to then determine the level of oversight that's required on each vendor relationship.

Download free samples of control assessments and see how Venminder can help reduce your third-party risk management workload.

Download Now





venminder

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

(270) 506-5140 | 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, vendor risk 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.