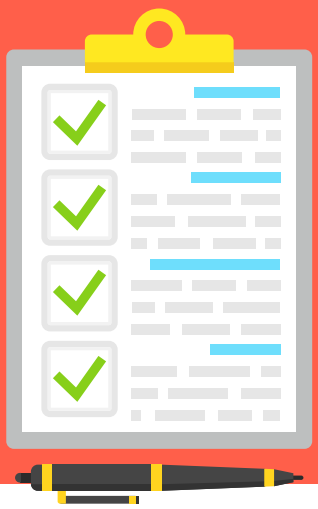
Creating a Proper Vendor Risk Assessment Questionnaire

venminder

Creating a Proper Vendor Risk Assessment Questionnaire



Understanding the risk, whether for new or existing third party products or services, often starts with a questionnaire. Frankly, creating a questionnaire in and of itself can be quite a large task. You can start with either an industry standard questionnaire, such as the SIG or SIG Lite, or create your own questionnaire.

Creating a Vendor Risk Assessment Questionnaire

There is no set format for a risk assessment or questionnaire. The regulatory guidance, while fairly prescriptive, doesn't provide a handy template; 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:

Always consider the regulatory expectations.

For more information on what factors you should consider, the FDIC and OCC have a couple of resources - FDIC Letter 44-2008 and OCC Bulletin 2013-29 - that outline categories of risk that must be addressed depending on the service or product being provided.

2

STEP 2:

A best practice is to always determine a rating system.

This is so you can effectively score and report on the various categories of risk based on the information you receive from your vendor. It's encouraged as a best practice to always determine the business impact and regulatory risk. Business impact risk determines if the vendor is critical or non-critical to the organization. Regulatory risk often determines if the risk is low, moderate or high. What you call these ratings and the number of risk levels can vary by organization. Remember, you will have both a business impact AND regulatory 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 to develop the questions that will be included in the vendor risk assessment(s). The following are recommended questions to determine the ***business impact risk***:

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. Would the time to recover normal operations exceed one business day?

If you answer **YES** to any of these questions, then you should consider the vendor to be critical. Now that you've determined if the vendor is critical or non-critical to the organization, it's important to consider the regulatory risk.

To determine ***regulatory risk***, you'll review several categories of risk. The categories considered will vary dependent on the products or services being provided. ***Per FDIC Letter 44-2008, some of the most common categories included are:***

1 Strategic Risk

This risk is present if the third party is used to conduct company functions or offers products and services that are not compatible with your organization's strategic goals, can't be effectively monitored by the organization or does not provide an adequate return on investment.

Example of a Question to Consider:
Are the vendor's products or services consistent with the organization's existing services?

2 Reputation Risk

This risk is of concern when the third party interacts directly with your customer. If the relationship does not meet expectations, a reputation risk can be posed to your organization.

Example of a Question to Consider:
What is the vendor's complaint volume?

3 Operational Risk

This risk occurs in all products, services, channels and processes when it's critical to your organization's operations.

Example of a Question to Consider:
Is sensitive data, such as non-public information (NPI) or personally identifiable information (PII), being exchanged?

4

Financial/Credit Risk

A third party's financial posture is important to keep in mind as a decline in financial condition can impact the overall relationship.

Example of a Question to Consider:

Has the vendor ever filed for bankruptcy?

5

Regulatory/Compliance Risk

Evaluating this risk helps you better understand the third party's adherences to laws, regulations, guidelines and industry specifications.

Example of a Question to Consider:

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

6

Transactional Risk

This risk occurs if there are issues with the service or product delivery.

Example of a Question to Consider:

Does the vendor process transactions on behalf of your organization, customers or employees?

**The above does not represent a list of all categories or questions to be included. The examples are provided as a snippet of what is recommended to be included and does not 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

A SIG and a SIG Lite are great resources to use, but they require you to be a member of the Shared Assessments Group in order to issue out the actual questionnaires, so you may need to consider developing your own questionnaire.

Questionnaires by Product or Service

Now that you further understand the steps to creating a vendor risk assessment questionnaire, **a note of caution** – with scores of different types of products, services or companies, you could come up with an endless array of questionnaires and that would be very confusing and nearly impossible to manage.

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

With that being said, *one size does not fit all* and that should not be the only approach taken. After all, do you really want to ask the landscaping company about the SSAE 18 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 will 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. Tailor your assessments and follow-ups to the vendor as deemed appropriate.

As you receive answers back from questionnaires, ensure you're not getting simply "Yes", "No" or, worse yet, "it depends". It doesn't give enough information in most cases. And, you should thoroughly document the risk assessment to show the basis for the analysis and rating you assign.

In the Venminder software, as a best practice standard **we have created three levels of questionnaires, ranging from 39 questions up to about 100 recommended questions** to include, with room to customize as much as you'd like.

Inherent vs Residual Vendor Risk

You must understand the inherent vs residual risk when completing a vendor risk assessment so that it's properly done.

Inherent Vendor Risk

Inherent risk is the risk present upon first impression, meaning the risk you notice immediately. For example, if you review the vendor's financial statements and quickly notice a rapid decline in financial condition over the last 3 years, then there's inherently a high financial risk present. Once you've discovered an inherent risk, you must work to mitigate, or reduce, the risk as much as possible. You can do that by:

- Documenting the controls and processes that should be in place to mitigate the risk, the scope, frequency and why
- Considering if you need to request that the vendor contractually commit to delivering these controls

Residual Vendor Risk

Residual risk is the risk that is still present once all efforts to control, or mitigate, the inherent risk have been made. It should never equate to more risk than what was initially found. Often, by mitigating the risk inherently present you'll be able to reduce the risk level (i.e., from high to moderate or from moderate to low risk).

In other words, inherent risk is what you first encounter and residual risk is where you've come to terms that you're comfortable you've got the right controls in place to reasonably mitigate any risk that is present.

Can a Vendor Assessment Go Overboard?

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

A few reasons why a risk assessment can go overboard:

- You haven't properly researched the vendor, or the products and services being provided, and you're using the wrong assessment to evaluate the risk level (i.e., there are too many questions that do not pertain to this type of vendor relationship).
- Your vendor assessment is too detailed or inconsistent with the risk presented by the vendor.
- Your risk assessment reaches the wrong conclusion or final risk rating.
- Your risk assessment is so comprehensive that business owners don't understand it or won't help to complete it.

Vendor Risk Assessments Lead to Proper Oversight

Creating and completing a vendor risk assessment can be a very cumbersome task that may take several iterations, but it's a vendor due diligence step that should not be taken lightly. Keep in mind, risk assessments 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 assessment is your go-to resource to determine the level of oversight that is required on each vendor relationship.

If it's determined that a relationship is high risk or critical once you've completed an assessment, you are now more prepared to mitigate risk and are more aware that the due diligence performed needs to be increased. A few extra precautions that many organizations take include more frequent monitoring, annual performance assessments and including additional considerations in the contract.

It's also a regulatory expectation to keep senior management and the board as informed and involved as possible, particularly as the risk changes. By completing thorough vendor risk assessments, you have obtained results that can be shared to keep them aware, which will lead to more effective communication across your organization.

venminder

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

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.