How To Do a Vendor Risk Assessment

Performing a vendor risk assessment can seem daunting, but it's a worthwhile time investment and necessary component of a third-party risk management program. You don't know the risk elements and level of risk associated with a vendor until you do one.

The tried-and-true steps to completing a vendor risk assessment...

1 **Determine criticality.** This determines how essential a vendor is to your business. A few examples of helpful criteria to identify a critical vendor are:

- *A disruption in service would cause a material impact to our organization or customers.*
- *The product or service supports a significant revenue stream.*
- *There's a significant expense necessary to implement/manage the vendor service and/or replace the vendor if need be.*
- *If the vendor service is disrupted for more than 24 hours, there will be a negative impact on our operations.*

2 **Determine the inherent risk.** This is the most risk possible in the vendor relationship before taking any action to reduce the risk present. A few sample questions that can be used to determine inherent risk are:

- *Will/does this product or service in any way impact our customers?*
- *Is sensitive data being accessed by this vendor? If so, will they be hosting it themselves?*
- *Will/does the vendor process financial transactions on our behalf?*
- *Do we rely on this product or service to maintain compliance with any regulatory guidance?*
- *Will/does this product or service require a significant expense?*

3 **Decide how to handle risk.** Once you determine the inherent risk and criticality, decide next steps. These are **four** of the primary risk-handling techniques:

- **Avoid** *the unnecessary risks completely by not using the vendor.*
- **Mitigate** *the risk by implementing or identifying the controls that are already in place. A control can be an action, process, strategy, task or requirement that aims to "prevent" and/or "detect" risks.*
- **Accept** *the exposed risks with approval from appropriate leadership and stakeholders. This should be well-documented and justified.*
- **Transfer** the risk by establishing insurance policies or contractual terms.

Avoid | Mitigate | Accept | Transfer

4 **Collect vendor due diligence.** Request pertinent information from your vendor as it relates to the inherent risks. You can request any applicable audits, certifications or reports which help you understand their control environment.

Collect

5 **Assess vendor information.** Experienced personnel should thoroughly review the required vendor documents to determine the mitigating controls are sufficient.

Assess

6 **Establish internal controls (as needed).** Vendors aren't solely responsible for protecting your organization from risks. Here are two internal controls examples:

- *Pertinent information security controls (i.e., access management, encryption and secure data transfer)*
- *Appropriate training that reduces or avoids unnecessary vendor risk*

Document

7 **Determine residual risk.** This is the remaining risk after you've taken steps to implement risk controls and the rating should be within the acceptable parameters of your organization's risk tolerance.

Residual Risk

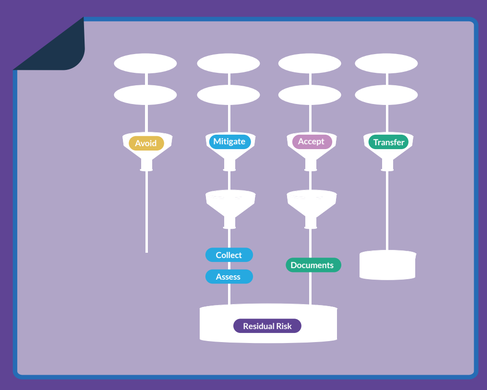
After the Risk Assessment

8 **Schedule ongoing monitoring.** First, address any unresolved issues or control weaknesses that require remediation. Then, be sure that the relationship is appropriately monitored throughout the term of the contract. Monitoring may include: SLA tracking, subscribing to third-party monitoring tools (i.e., Argos Risk, SecurityScorecard, BitSight) or circling back to reassess this vendor on a periodic basis.

A good standard for the frequency of periodic risk assessments would be:

- **Inherently high risk or critical:** *Annually*
- **Inherently moderate risk:** *Every 18 months - 2 years*
- **Inherently low risk:** *Every 3-5 years*

9 **Document and report.** After your assessment is complete, be sure your findings are well documented and reported to the appropriate people.



Vendor risk assessments can provide your organization with the information needed to make sound and informed business decisions, minimize the likelihood of unexpected negative outcomes and manage processes practically and efficiently.

PRINTABLE VERSION

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.

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

Copyright © 2022 by Venminder, Inc.