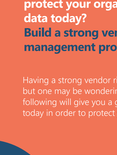
Creating a Vendor Risk Management Program that Protects Your Organization

It's 12:00 am.

Do you know where your data is?

That has become the question today, as the risk of not knowing is too great.

Organizations must be able to answer the following:



1. Where is their data located?
2. Who has physical possession of their data?
3. Who has logical access to their data?

With absolute certainty, in order to protect your organization, you must know how any third-party vendor is going to utilize your data.

Managing the multi-faceted risks that vendors pose to any organization today is a daunting task. However, not knowing what your third-party vendor is actually doing with your organization's data, or when a fourth-party vendor may have access to your data, can lead to a significant increase in your organization's risk.

What do you need to do to protect your organization and data today?
Build a strong vendor risk management program.

Having a strong vendor risk management program is a great place to start, but one may be wondering what a strong program would entail. The following will give you a good idea of what your program should look like today in order to protect your organization.

5 Critical Elements of a Vendor Risk Management Program

1. The Board

It all begins, and ends, with the board. Regulatory guidance tells us that the board must be actively involved in an organization's vendor management program. The board should provide you with a formal risk appetite statement to start with and that you can then build upon.

2. Senior Leadership

Once the overall risk appetite has been determined, senior management must be actively engaged in the vendor management program. They must be involved when it comes to your critical third parties; particularly those critical third-party vendors with access to your data.

3. Lines of Defense

Your lines of defense play a critical role in overall third party risk protection at your organization. "Lines of Defense" is a short-hand way of referring to the layers your organization probably already has in place, and how they can work together to help mitigate your organization's risk.

Here's how and why:

First Line – This is comprised of your employees in your business units who interact with the vendor every day. They're the best resource for up-to-the-minute intelligence on any vendor issues or potential problems. They'll probably be the first to know how the vendor is handling your data and what they're doing with your data. Knowing will enhance your vendor due diligence and lower your risk.

Second Line – This is typically your vendor management team. They can escalate and draft board overviews, if needed.

Third Line – This is the internal audit and compliance departments who ensure everyone is following regulatory guidance, as well as internal policies and procedures. They make sure the appropriate precautionary steps are being taken to protect your organization from risk.

4. Strong Governance Documents

Implementing strong governance documents, such as policies and procedures, is important. Within your vendor risk management policy, be sure to define the program's overall objective and vendor risk framework. Keep the policy relevant to your goal, which is protecting everyone involved and your organization from vendor risk while in accordance with regulatory guidance.

5. Strong Program

Develop a program that encompasses the 7 stages of the vendor risk management lifecycle. By following these stages closely while working with any of your vendors, you're greatly limiting the amount of risk that your organization will be exposed to. This is because each of these lifecycle stages help to work as a "catch all" to discovering any risk that may have gone unnoticed otherwise.

The Seven Stages

1. Planning – This is the first stage of the vendor risk management lifecycle and involves developing your governance documents, detailing how you'll provide vendor oversight.

2. Risk Assessment – Complete a risk assessment on every vendor, both during due diligence & third-party selection and as part of ongoing monitoring.

3. Due Diligence & Third-Party Selection – This means properly vetting every third-party vendor. Pre-contract, obtain and review all due diligence and conduct risk assessments to evaluate the risk posed to your organization.

Quick Tip: Start vetting before you watch the webinar or agree to a demo!

4. Contract Management – This includes negotiating the contract terms and ensuring compliance, change management and ongoing maintenance of the relationship.

5. Ongoing Monitoring – Continuously monitoring vendors with access to your organization's data is mission critical. Request updated due diligence, perform ongoing reviews and risk assess throughout the entirety of the contract.

6. Exit Strategy – You can't simply terminate a vendor relationship and be finished. Often, you don't completely know where your data is being stored or who's working on it. Exit strategies must be identified and included in your vendor contracts.

7. Termination – It's after following your exit strategy that you can move the vendor out of the lifecycle and terminate the engagement, if needed.

Remember, we trust but verify when it comes to data.

Build out the verification process and know how data return or data destruction will be conducted by incorporating expectations into your contracts. Ultimately, you're protecting your organization by having a well-developed vendor risk management program that incorporates strong data protection plans.

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

DOWNLOAD NOW

PRINTABLE VERSION

venminder

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

(270) 506-5140 | venminder.com