COVID-19 SHINES A LIGHT ON THE IMPORTANCE OF THIRD-PARTY RISK MANAGEMENT

Have You Had the Third-Party Risk Management Light Bulb Moment Yet?

COVID-19 has increased risk within all facets of an organization, especially with vendor relationships. Therefore, it's important now more than ever to have a solid third-party risk management program in place.

What Is Third-Party Risk Management?

Third-party risk management is the process of fully identifying all of the significant companies that aid in the delivery of a product or service to an organization or to an organization's customers on behalf of the organization. It involves controlling costs, driving service excellence and mitigating risk to gain increased value throughout the whole lifecycle.

Why Is Third-Party Risk Management Important and Especially Now?

Here are 6 reasons:

Strategic and Security Advantages
A good third-party risk management program creates real strategic and security advantages as you're able to ensure you have proactively addressed potential vendor concerns – running the gamut from preventing data breaches, avoiding reputational risk issues, ensuring solid business continuity plans between you and your third parties and perhaps even reaping some cost efficiencies. And, within the business continuity plan is pandemic planning. These days, strong pandemic planning has become a vital component of an organization's success.

Comprehensive Risk Mitigation
To ensure the safety of your organization, you must mitigate risk of all kinds. Having all the necessary information before you even begin a vendor relationship is critical, but the work doesn't stop there. At a time like now, for many vendors, financial strains and risks are only increasing so you always want to know your vendor's viability. That requires a good third-party risk management program that includes comprehensive, ongoing risk mitigation. Third-party risk management is all about what you continue doing to make sure your organization can continue operating at its best and ensuring your vendors are there to support you at every step of the process.

Complex Vendor Networks
Depending on the size of an organization, it's not an overstatement that some organizations work with hundreds or even thousands of vendors who also have their own cast of subcontractors and partners. This only multiplies an organization's risk. Without a solid oversight program, third and fourth-party risk (and so on) can easily get out of hand. It gets increasingly complex when you think about all of the places that your customers' data can flow. To make the data flow even more complex, now many of your vendors' employees are working remotely which could increase the odds of a data breach if there are flaws in their information security procedures and networks.

Regulatory Requirements
Without alignment with regulatory rules and requirements, an organization could end up facing steep non-compliance fines and penalties. Regulatory risk is at an all-time high. Putting even more emphasis on the importance of managing third parties, the FFIEC's Interagency Statement on Pandemic Planning mentions critical third parties numerous times. And the FDIC recently updated its Risk Management Manual of Examination Policies which includes changes to Section 21.1, Emergency Planning, to address COVID-19 related modifications.

Complicated Vendor Monitoring Processes
Because vendor networks are often so complex, monitoring these relationships can be equally challenging. A centralized, scalable third-party risk management program helps streamline the vendor management process, and ultimately helps you keep tabs on the vast amount of information required to maintain a healthy risk management system.

Policy Awareness and Training
Ongoing training is an integral part of ensuring compliance and mitigating risk. Many organizations fail to incorporate vendor risk within their own internal training programs, which can result in a rash of human error leading to unnecessary risk exposure and operational issues. Furthermore, a well-functioning and documented risk management program can help close the gap between organizations and their vendors to better manage both compliance and risk.

Ways to Improve Your Third-Party Risk Management Program

If your organization's program isn't exactly where you want it to be, there are places to make small adjustments that'll have a big impact on both the maturity and operational acuity of your current third-party risk management program.

Here are 5 tips to help:

1. **Follow the third-party risk management lifecycle**
This is an important best practice that can be used for every vendor relationship. A vendor relationship should always go through the following phases during the entire partnership: planning, risk assessment, due diligence & third-party selection, contract management, ongoing monitoring, exit strategy and termination.

2. **Collect and assess vendor due diligence**
Collect vendor due diligence and then take it a step further by assessing the documentation. This'll help you further understand your vendors' processes and any risks posed to your organization and customers. Here are some of the important items you should be reviewing now, especially with the pandemic:
   - Financials
   - Business Continuity and Disaster Recovery Plans (this includes pandemic plans)
   - Information Security Policies and Procedures
   - Cybersecurity Plans
   - SOC Reports
   - Vendor Complaints (Tip: you can check out the CFPB complaints database or complaint websites to help with this)
   - Remote Operations Plan or Policy

3. **Review your vendor contracting policies and procedures often**
The contract is a key component of every vendor partnership. If it's not in the contract and if individual accountability isn't assigned, it won't happen. Therefore, contract management must be strong.
   Here are 4 contract oversight recommendations to get you started:
   - Include right to audit provisions in the contract
   - Create a robust method for tracking significant dates so that an important one doesn't go unnoticed such as a non-renewal notice period
   - Keep your contracts in one centralized location for ease of access and consistency
   - Include data handling and data destruction guidelines

4. **Develop a set of governance documents, such as a policy, program and procedures**
These should be reviewed at least annually, but more frequently if something like the following occurs:
   - A change in your organizational structure or best practices
   - New regulatory guidance needs to be cited

5. **Involve senior management and the board**
Regulation requires they stay involved by doing things like the following:
   - Review and approve your governance documentation at least annually
   - Review all activity pertaining to critical and/or high-risk vendors
   - Determine the risk tolerance of the organization

The regulatory environment for third-party risk management was already becoming increasingly complex with the rising growth and complexity of vendor networks, and now, there's added increased risk from the pandemic.

An organization's approach to third-party risk management can have a significant impact on both its success as well as its security.

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

DOWNLOAD NOW

PRINTABLE VERSION

venminder

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

(270) 506-5140 | venminder.com