TWCA | Risk Management Fund

# Vendor IT Risk Management

Vendor risk is an important part of any corporate risk management strategy. Companies today rely on an overwhelming number of vendors and suppliers from all over the globe. This allows businesses to be vulnerable to severe disruptions caused by serious events affecting service providers, such as bankruptcy, disasters, and data breaches.

Vendor risk management identifies and mitigates the risks of outsourcing to third-party vendors or service providers. For example, third parties might have access to an organization's personnel information, finances, security procedures, client data, or other sensitive information. Research and due diligence are key to understanding a third party's information security structure and if they are adequate for the specific job assignment. Unfortunately, this type of due diligence is an ongoing process. Communication, assessment, and monitoring should be performed during the entire relationship with the third party.

So, what are the risks to look for with third-party management?

**Financial Risk**
This type of risk relates to contractors failing to achieve financial performance goals. This can be seen in the form of cost overruns and expenditures that don't align with contract terms. Find out which contractor has the most influence on the bottom line and provide consistent attention to those operations.

**Cyber Risk**
Third-party vendors are not strangers to having their operations exposed by misconfigurations and therefore becoming the target of threat actors. When an organization has multiple vendors, the stakes are risen. Assessments of vendors should include the following:

- Has the vendor been breached in the past?
- How the third-party maintains an organization's data?
- How does the third-party connect to maintain an organization's systems?
- Is the vendor responsive?

**Compliance Risk**
Compliance and regulatory risk arise when an organization's business activities violate laws, industry practices, or regulations. These rules must also be reflected in the internal policies and processes of the organization. Laws are constantly evolving and vary from industry to industry. Depending on the type of vendor and the task assigned to them, different laws and regulations apply. It's crucial to ensure vendors follow the relevant laws,

rules, regulations, policies, and ethical standards because non-compliance can lead to significant fines.

**Reputation Risk**

Third-party vendors can harm an organization’s reputation in several ways, including interactions that don't meet your company's standards, handling any sensitive data with carelessness, or failure to comply with legal and regulatory requirements. The public's impression of your organization matters significantly because it can influence customers and your entire business.

From vendor selection to onboarding to completion (and beyond), vendor risk management helps identify the risks your third-party relationships pose to your organization. You can work directly with vendors to remedy those risks and continuously monitor for changes in your vendors’ risk posture that could affect your organization.

The TWCARMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments and Incident Response Plan Tabletop Testing visits for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor, by phone at 512-619-1437 or by email at Lee.Cain@sedgwick.com.