Demystifying Vendor Risk Management

By Tom Strickland, Director and Tom DeMayo, Partner

In today's IT landscape, it is not uncommon to utilize a third party to support your operations. Be it a cloud provider, parts manufacturer, payroll processor or a law firm to guide you in regulatory matters. All these third parties have one thing in common: you as an organization entrusted them with your data or to support your operations.

With trust comes an expectation of performance that they will provide the services agreed upon in a responsible and secure manner. As Ronald Reagan once said, **"*Trust, but verify*."**

Due Diligence

As a business, you can't simply rely on the promise of a vendor. It is your responsibility to verify that any vendor you engage is up to the task and has the proper controls established. When your stakeholders or customers entrust you to perform a service, they are implicitly trusting anyone you engage in supporting the service will have processes and controls equal to or greater than yours. To accomplish this and uphold your responsibility of due care, a third-party due diligence and management program must exist.

Creating and overseeing a legitimate vendor management program is essential to organizations regardless of industry, service line or size. While not all third parties will have the same level of criticality or risk to your business, without managing and monitoring those third parties, how would you know and confidently ensure your stakeholders that you have provided your services prudently and exercised due care?

The following key steps are important to create a sound vendor management program.

- Know who your vendors are. Inventory all your vendors and document the services they provide.
- Risk rank your vendors. If they are operationally critical or are entrusted with sensitive data, they are a high-risk vendor. High-risk vendors require the highest level of scrutiny and due diligence. Moderate to low-risk vendors require a level of due diligence; however, the extent and frequency of due diligence will not be as intensive or frequent as a high-risk vendor.
- Assess your vendors. Once your inventory of vendors has been risk ranked, the next step is to define and implement a process for assessing vendors. This may take the form of an established due diligence questionnaire or the request and review of various documents and reports they may provide, such as a Service Organization Control Report (SOC).
    - A word of caution on SOC reports. In our experience, many organizations falsely presume that just because an organization has a SOC report, they are satisfactory. That assumption is the farthest from the truth. A SOC report tells a story; however, the story may not always be positive. It is important that the organization scrutinize the SOC report to determine if the report has a satisfactory opinion from the audit firm and that the report clearly describes the services provided, the controls established and the auditors' testing is sufficient to support their conclusion. Unfortunately, having a report is not indicative of

sound controls. It is not uncommon to obtain reports that are generic and don't speak to the services and risk of the third party's operations; as such, additional questions and follow up must occur.

- Ensure that any new vendors are assessed *prior* to contract execution. Many organizations struggle with this as departments procure cloud-based applications with no input or validation from IT. This is often a byproduct of department heads assuming that because IT is not needed to facilitate the deployment, they do not need to be informed. If data or technology is involved, IT should have input.

- Based on the results of the due diligence, include necessary provisions to ensure the vendor is accountable for the protections and controls they promised. Should they be breached, an agreed-upon timeline of notification to the business should exist.

Questions Answered

The end result of your due diligence should provide answers and, hopefully, comfort in answering the following key questions:

- Are governance controls established, such as policies, standards, risk management and awareness training?

- Is the technology stack sufficient to support the services outsourced?

- Are the security controls well defined to ensure the confidentiality, integrity, availability and privacy of the information they will be entrusted with?

- Do they comply with any necessary regulatory and legal requirements the business is subject to? For example, if the organization has privacy obligations under state privacy laws such as California, does the vendor have the necessary controls themselves to handle the data in a manner consistent with the privacy policy established by the organization? Whatever you as a business promise in your privacy policy must flow down to any vendors you utilize as part of the services provided.

Building a sound vendor management program is a process that requires effort and resources to do it correctly. It's also important to think about the different ways a vendor can impact an organization's business.

Contact Us

Does your organization have the right resources and expertise to manage third-party vendor risk? PKF O'Connor Davies can help answer your questions and lay out a practical approach to vendor management. For assistance, contact your client account team or either of the following:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Tom Strickland, CISSP, CISA
Director
Cybersecurity and Privacy Advisory
tstrickland@pkfod.com | 781.937.5305