NAVEX™

Checklist

IT Third-Party Risk Management Getting Started Checklist

In today's interconnected world, organizations of all types rely on third-party vendors for raw materials, components and services that are critical to fulfilling their core missions. In the case of an organization's IT function, these third-party vendors can consist of suppliers of servers, computers and other hardware, and service providers for internet, phone, software-as-a-service, cloud storage and more.

While this reliance is nothing new, efforts to streamline internal operations and reduce costs by focusing on scalability have led to a dramatic increase in the use of third-party vendors over the last 20-plus years. This shows no signs of slowing down. While third-party vendors can tremendously help companies grow and scale, they also create risk for both the IT function and the organization at large such as operational risk, reputational risk, cybersecurity risk, and more.

Therefore, regardless of their size or the number of vendors, IT areas need a comprehensive process to proactively identify, assess, monitor and mitigate risks emanating from third parties that goes beyond the basics of reviewing contract language and pricing.

IT Risk Spans Well Beyond IT Function

Not only is increased reliance on third parties leading to a higher number of risks, the impact of these risks is being felt not just by IT but throughout the company. IT managers who fail to take steps to address these risks could be exposing not just their functional area, but their entire company to heavy losses – especially considering that many of these risks are intangible and thus uninsurable.

It is these risks that make IT third-party risk management so important, especially considering that a greater share of an organization's value is driven by intangible assets like reputation.

If a vendor is engaging in unethical business practices or has lackluster cybersecurity that puts customer data at risk, this could reflect poorly on IT and the entire organization, potentially leading to inquiries from regulators and a barrage of negative attention from the press and social media.

If a particular service provider suddenly went "offline" without warning, the impacts will inevitably spill over, impacting operations across the organization. Customers who depend on the organization's products and/or services will not differentiate between the company and the third party. They will instead seek out alternatives if these issues materialize, because after all, the customers have people and other businesses who rely on them.

These are just a couple of situations that illustrate the importance of IT third-party risk management, but with supply chain disruptions and other shortages seemingly becoming part of everyday life, IT departments and their organizations have even more reason to take proactive steps to ensure they have the resources and services needed to serve those who depend on them. Saying "this is how things have always been done" will no longer be an acceptable answer in today's tumultuous world.

Unfortunately, only a small portion of IT departments do this well, as many IT leaders believe it is too difficult or time-consuming.

A journey of a thousand miles begins with a single step – the important thing is to get started.

Continue reading for five steps IT managers can take to begin mitigating and managing the inevitable risks that arise with using third-party suppliers and service providers.

IT leaders and staff should not expect a robust process that helps address all third-party-related vulnerabilities to magically spring up in an instant. Any risk management process involves trial and error and has room for improvement, but the following five steps are a great springboard to developing a process that works for a specific organization's IT department.

1 Assess critical needs by identifying areas needing immediate attention

Absent a blank check from upper management, it is impossible to carefully examine each vendor immediately. Therefore, in these early stages, IT managers must separate the vendors deemed most critical to helping the company achieve its strategic goals or conduct basic, essential operations. Carefully examine previously reported complaints or identified issues to understand where systems and processes need shoring up. Technology audit reports can serve as a useful source to prioritize where efforts will first be spent.

As an example, a payment processing company will rely heavily on IT, specifically internet services, for fulfilling its core mission. Without a functioning network, merchants will not be able to process debit and credit card payments, which could therefore wreak havoc for countless numbers of businesses and badly damage the reputation of the processor as a reliable partner.

2 Build the business case for vendors based on strategic objectives or business processes

Understanding the "why" behind something is one important step for ensuring the best decisions are made. This is especially true when it comes to vendors, so it is therefore imperative that IT take these steps. When initiating a relationship with a third-party, a few questions that IT managers and risk professionals should be asking include:

- When did the company first identify the specific need to engage with this third-party or use this service/product?
- What events led to this need to procure product(s) or service(s) from the third-party?
- What are the specific strategic objective(s) or business process(es) this particular vendor will help IT and the broader organization fulfill? Provide detailed explanation.
- Are there any existing third-party relationships that can adequately fill this need?
- What is the anticipated cost of the entire contract and was this included in the current year's budget?

With this information in hand, IT can then determine not only if the level of risk aligned with the particular vendor is justified in relation to the specific goal(s) the relationship is intended to address, but also the risk(s) of opting not to engage with this vendor.

3 Collaborate with other business units to understand their needs

Randomly performing third-party risk management, especially for IT, is not going to work in a vacuum, especially when it comes to an IT function that so many other areas of the company rely on. Any mitigations or other activities done without coordinating with other business areas may end up creating additional risks to or causing problems for the company.

Therefore, it is imperative to sit down with business areas across the company to understand their critical needs and how IT helps meet those needs. For example, a customer service or tech support unit will rely heavily on internet-based voice chat, which means reliable internet service is a requirement. Shoring up this particular vendor and developing a quickly deployable alternative is one way IT can help ensure continuity for this particular area.

4 Examine the entire supply chain by understanding vendors' vendors

This may seem like overkill in the early stages, but examining vendors of any third parties (also known as fourth- and fifth-party suppliers) is crucial to gaining an overall picture of a company's third-party risks. Reports have been consistent of companies having trouble procuring vital raw materials for manufacturing their particular products.

In the case of IT, both hardware and software providers will have other vendors they rely on.

Computer chip shortages have led to backorders and delays for laptops, servers and other components necessary for an IT department to function. Disruptions in the supply of copper could easily spawn shortages in network cabling, or a SaaS provider could be relying on a cybersecurity service provider that fails, leading to company data being compromised.

Taking proactive steps to understand who vendors rely on for raw materials or critical services can allow for alternative sources to be developed and deployed the moment trouble is brewing. If an alternative is not available, another couple of options include: one, add contract language requiring a third-party to diversify its suppliers; or two, require the supplier to obtain a surety bond, which is essentially a retainer paid to a bond company that in turn guarantees a contract will be fulfilled.

5 Assess risks with specific vendors

Once the critical needs are handled, it is time to move into more long-term, risk-based due diligence around current and future vendors. Since this is the process that will be used over the long-term for evaluating vendors, there will be considerable trial and error to arrive at an effective process for the IT department.

One important part of this due diligence process is categorizing vendors between commodity, significant, and critical, or whichever terminology works best. A commodity vendor is one that is easily replaceable. A significant vendor is replaceable but doing so does require more effort and planning than the replacement of a commodity vendor. Critical vendors cannot be replaced without a hefty time, money and people resource investment, and will therefore likely require more attention.

In the long-term, this assessment, categorizing, and ongoing due diligence will drive the amount of time spent on relationship management and oversight. Without this step, it is highly likely that a vendor that ultimately does not require much attention will receive too much, and vice versa. This process helps ensure IT is focusing on the right vendors in the right way at the right frequency.

This area also presents many opportunities to automate, which is highly recommended as much as possible to save time for IT leaders. Whether it is gathering documentation from a vendor based on contract requirements or setting automatic triggers – automated activities can be established with triggers and reminders between activities to avoid overlooking steps. This also helps team members to have a predictable workflow they can factor into their schedules. Building workflows supported by systems as much as possible helps ensure an efficient third-party risk management process.

Next Steps to Implement IT Third-Party Risk Management

The five steps outlined here are just a beginning. Remember, this is an iterative process that will require some trial and error. There will always be room for improvement, but as programs mature, more advanced ways of managing risk become available.

Every company and every department within a company, including IT, relies on third parties, and these third parties can absolutely introduce new risks to the organization.

Taking proactive steps to understand these risks and mitigate their impacts to the organization will help IT managers and executives make better-informed decisions and not be caught unaware in the event a risk materializes.