How your board can oversee third-party risk

Products and services provided by third parties are critical to business today. But they can also bring big risks.

October 2020

Given the sheer number of third parties that companies rely upon, it’s important to evaluate and manage the related risks. Boards can play an important role in setting the tone by encouraging management to establish effective third-party risk management programs.

pwc.com/us/governanceinsightscenter
All companies rely on third parties to some extent. While some have only a few third-party relationships, others have thousands. They can help companies save costs, improve service speed, and provide global access. They can also allow companies to be more flexible and competitive.

But third parties can also pose risks, from reputational and brand risk to the risk of serious financial damage. This means companies need to carefully select and proactively manage and monitor third parties and associated risks. We’re not just talking about obvious problems like bribery, fraud, and legal compliance. Some vendors access or store a company’s intellectual property, records, data, and network—raising cybersecurity and data privacy issues. Others manufacture on a company’s behalf, and can bring worker safety and human trafficking issues along as a result. And the implications go on.

The number of third-party relationships a company has can be staggering. In our experience, companies underestimate the number they interact with by a factor of three to five. While third-party management may get more attention at organizations in certain regulated industries or when there have been regulatory issues (e.g., Foreign Corrupt Practices Act), the risk extends beyond those circumstances. All companies do some kind of business with third parties. Understanding the complexities of those relationships can be challenging.

So how can boards make sure there’s enough focus on third-party risk management before problems arise? Here we answer this question as we explore the basics of third-party risk.

What do we mean by a “third party”?

In this context, a third party is any individual, company, customer, vendor, supplier, agent, or distributor that interacts with or on behalf of a company. Third parties can provide all types of services, from processing payroll to running data centers. Some companies use third-party local country experts, lobbyists, or joint venture partners to drive business in new locations. Often, third parties also have their own vendors.

21% of organizations have no third-party due diligence or monitoring program.

What role should the board play given their risk oversight role?

First, determine which board committee will cover third-party risk. While the full board should understand management’s process for addressing this risk, it’s common to delegate day-to-day oversight to a committee. Boards with risk committees commonly task that group with oversight. Many other boards allocate risk oversight responsibilities in general to the audit committee. Regardless of the committee that has responsibility for oversight, the full board needs to understand how management is addressing this risk.

The board should start with understanding how the company leverages third parties. This might highlight the significant third parties that are integral to the company’s delivery of their business strategy. While the company will be responsible for establishing third-party diligence processes and monitoring risk, the board should understand what that entails. To do this effectively, the board needs to understand the risk landscape and get comfortable with the program and the processes. Boards need to understand the challenges involved in managing third-party relationships and what an effective third-party risk management program might include.

Boards might also want to think about the impact of third parties as they consider enterprise risks and whether internal audit should perform an annual review of the key controls associated with a third-party risk management program.

Depending on the maturity of the organization’s third-party risk management program, the board should seek periodic updates from those in charge. The nature and depth of reporting from management to the board will look different from company to company and doesn’t necessarily mean the board should receive frequent, detailed lists of vendors. The goal is for boards to understand the third-party risk landscape for their companies and to get comfortable with the related programs and processes.
What are the hurdles to understanding third-party management risks?

Getting a handle on a company’s third-party relationships can be overwhelming for several reasons. To have a deeper discussion with management on the topic of third-party risks, the board should consider these areas of concern.

Lack of an inventory of third-party relationships

The vast number of third parties many companies have makes it tough to inventory even the ones the company works with on a regular basis. Companies may not know who all their third parties are for several reasons. For one thing, managing third parties is often siloed. Also, many countries rely on historical relationships. Plus, in some cultures, businesses rely on a person’s word or handshake and so there may not be contracts or formal agreements at all.

Incomplete understanding of what third parties are doing

Companies often don’t have a centralized or real-time view of what their vendors are doing. Companies may also lack a consistent way to categorize or tag their third parties based on the service they provide. A vendor might have been approved for one use (say, processing certain data), so a manager may think it’s okay to use that vendor for something else (say, providing cloud storage). But different services should prompt additional evaluations—even for approved vendors.

Little appreciation for how third parties operate

Third parties may have key operations outside the US—in countries with significantly different business practices. Some of those may violate US laws, as well as contravene the company’s ethical culture and operating standards. For example, providing gifts and other incentives may be common practice in other countries to build—and maintain—business relationships. But those gifts may be considered bribes under US law.
The process to select third parties is flawed

Too often, when a company is engaging or evaluating a third party, the correct leaders are not at the table. As a result, the company may not have a complete understanding of all elements that need to be considered. For example, a company might bring on a third party to expand into another country without thinking about potential data-sharing risks.

Risks and rewards require balancing

Cataloging and analyzing a company’s third parties can also be expensive, particularly for companies that are starting from scratch. Often, there is little appetite to dedicate resources to such a process unless there is a specific need to do so. On the flip side, if there is an issue, the organization could potentially spend even more money to resolve the issue. Management must find the right balance.

The review and approval process takes too long

Shepherding a third party through a thorough evaluation and approval process takes time. Often, the business may be impatient to activate the third party—and it can be tempting to circumvent the process to expand into another country without thinking about potential data-sharing risks.

Assessing third-party risk

Which types of risks are common with third parties?

**Cybersecurity and data privacy**

Many companies use third-party vendors for technologies critical to the business. But often, companies don’t realize how many of their third parties could have access to sensitive data. Some companies have fallen victim to data breaches because of their third-party vendors—who are often targets because of their access to data or their insecure entry points. Plus, there are privacy laws to comply with, so companies need to consider how their third parties are staying on top of those requirements.

**Bribery/FCPA**

Every US company conducting or seeking business abroad is subject to the Foreign Corrupt Practices Act (FCPA). The FCPA’s anti-bribery provisions prohibit paying bribes to foreign officials to help get or retain business. That prohibition extends to the agents, distributors, and other third parties that work on a company’s behalf.

**Compliance**

There’s more for companies and their third parties to comply with than simply FCPA and data privacy laws. There are also anti-money laundering, and consumer and employee protection laws. There are also stringent industry requirements for certain sectors, such as for medical devices.
Ethical/Social/Environmental issues
As companies expand operations globally, many times in order to save on production costs, it can be very difficult to track a company’s complete supply chain. And that often opens ethical and social risks—and the possibility of a lawsuit or negative publicity.

Brand/Reputation
Consumers increasingly want to understand the practices of the businesses they interact with. In today’s always-on environment, unethical practices of third parties could go viral and turn into a brand crisis.

Operational vulnerability
A natural disaster or some form of cross-border trade restriction (think Brexit) that disrupts the supply chain can hinder operations. That’s especially true if alternative sources aren’t readily available.

Materiality
How much a company spends with a third party will always be part of the risk calculation. But the amount of spend isn’t the sole criteria. A third party that represents a relatively minor expense may present more significant risk depending on the nature of its services, such as with IT access.

45% of external actors identified as the main perpetrators of disruptive fraud are customers or vendors/suppliers of the company.

What does an effective third-party management program look like?

Establishing third-party risk management programs can be time-consuming. Boards will want to ensure that management is focusing the right resources for the risk. Critical elements of a third-party management program include:

- **The right leader.** This could be the chief risk officer or even the head of supply chain or some other global/operational function. Whoever is selected, that individual needs to have the ability to break down silos between functions and territories.

- **The ability to access resources across functional areas.** Assessing risk appropriately usually requires resources from IT, compliance, legal, HR, finance, cybersecurity, procurement, internal audit, and business units.

- **The discipline to assess each third-party relationship against a standardized third-party risk framework.** Identify the third parties the company deals with and understand the scope of the risk for each relationship using a standard evaluation framework.

Questions boards can ask about third-party risk

- Who has responsibility for the company’s third-party risk management program?
- What approach does the company take to perform due diligence on its third parties? Is an assessment made only at the beginning of the relationship? Or periodically to assess its long-standing relationships?
- How does the company monitor fourth and nth parties?
- Do vendor contracts include language requiring third parties comply with applicable territory and company regulations?
- How are internal audit and risk management involved in assessing the program?
In conclusion…

Using third parties is a natural part of the business landscape. Third parties provide companies with many benefits, but they also bring risks. The sheer number of third-party relationships companies often have makes it difficult to oversee the risks involved. That’s why having an efficient and effective third-party risk management program—including oversight from the board—is critical.
Contacts

Paula Loop  
Leader, Governance Insights Center  
paula.loop@pwc.com

Brian Schwartz  
Partner, Risk Assurance  
brian.schwartz@pwc.com

Catie Hall  
Director, Governance Insights Center  
catherine.hall@pwc.com