How your board can oversee third-party risk

Third parties are critical to business today. But they can also bring big risks.

August 2021

Governance Insights Center

Given the sheer number of third parties on which companies rely and with whom they collaborate it's important to evaluate and manage the related risks. Boards can play an important role by ensuring management has established effective third-party risk management programs.

All companies have third-party business relationships. Sometimes it's just a few, and other times companies 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 their 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.

Third-party risks grow—but so does dependence on third-parties

92% of businesses expect increased regulatory scrutiny of third parties

85% see their third-party risk exposure increasing

90% expect their dependence on third parties to grow

Source: PwC, *Building digital trust, US Digital Trust Insights Snapshot*, April 2021.

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, General Data Protection Regulation, the California Consumer Privacy Act), the risk extends beyond those circumstances. All companies do some kind of business with third parties—sometimes even with a collaboration agreement that doesn't include spending money. 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 explore the basics of third-party risk and how to manage it.

What do we mean by a “third party”?

In this context, a third party is any company, vendor, supplier, agent, joint venture partner, 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.

What role should the board play?

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 regular 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.

Next, 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.

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

Source: PwC, *Fighting fraud: A never-ending battle, PwC’s Global Economic Crime and Fraud Survey*, March 2020.

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. Boards can also ask about whether the company requested and/or received any additional assurance by external parties over controls and processes in place at the third parties.

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. 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.

Rising interest in external, independent assurance over third-party relationships

Companies often use questionnaires to gain insights on how third-party risks are managed. These questionnaires can be complex to create, manage, and assess, all while providing limited insight into the effectiveness of the processes at the organization. Companies also sometimes exercise their "right to audit" clauses and perform their own assessment of third-party processes and controls.

Companies can gain comfort over their vendors' privacy and security controls by requesting independent assurance over controls at the vendors. For example, companies can request SOC2 (Service Organization Controls) reports that are prepared by independent parties. These reports can be used to satisfy various company needs at the same time. SOC2 reports can provide independent assurance about whether or not vendors are in fact employing strong privacy and security controls over the data that the company has shared with them. Requesting and reviewing these reports from third parties provides multiple advantages: (1) there is assurance from an independent party about how the controls are operating (many third party risk management programs do not track whether or not the vendors' controls are operating effectively); (2) the company is better able to prove that it has a strong privacy and security program when a regulator or other legal body investigates; and (3) there is cost savings for the company because their resources will not be spent creating and reviewing questionnaires or doing onsite audits of the vendors.

What are the hurdles to understanding third-party management risks?

Getting a handle on a company's third-party relationships can be overwhelming. To have a deeper discussion with management on the topic of third-party risk management, the board should consider some of the complexities.

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 with whom 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. 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, possibly making it harder to track. There is also the practice of third-parties using their own suppliers, subcontractors, and other third parties to deliver products or services, referred to as "fourth" or "nth" parties. Companies may not have visibility to these "nth" parties and as a result leave them out of any tracking or inventory.

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. SOC2 reports can provide insight here because the reports describe the services provided and detail the controls embedded within the services.

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.

Materiality is not the sole focus

How much a company spends with a third party will always be part of the risk calculation. But the amount spent isn't the sole criterion. A third party that represents a relatively minor expense may present significant risk depending on the nature of its services.

The process to select third parties is flawed

Too often, when a company is engaging or evaluating a third party, the right parties 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 the process 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 in the interest of time, which increases the chance that risks will be overlooked or inadequately assessed.

Common third-party risk areas

Cybersecurity and data privacy

Companies may use third parties to access newer technologies (e.g., cloud, artificial intelligence, SaaS (Software as a Service), augmented or virtual reality) increasing their cybersecurity risk. They may also be sharing sensitive data with third parties. These risks come in both the form of privacy and potential security incidents, as well as non-compliance with an array of evolving and expanding regulations.

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.

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

Source: PwC, *Fighting fraud: A never-ending battle, PwC's Global Economic Crime and Fraud Survey,* March 2020.

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 to address 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. Whomever 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 and privacy, procurement, internal audit, and business units. Some organizations have set up third-party risk management offices to connect the risk across the company and streamline the process. Having a specific office can also help eliminate overlap and identify gaps.

A tailored approach to assessing risk

Organizations that use only a common questionnaire for all third parties likely miss the mark on the true risk each third party presents to their organization. Assessing risk for each relationship and determining the level of diligence allows companies to tailor needs to specific circumstances. For example, organizations with limited data sharing or reputational exposure may require a less rigorous oversight process than a third party with which you share large amounts of sensitive data.

An effective ongoing monitoring program

Only 54% of executives in PwC's *Building digital trust*: *Trust in third parties* survey state that they have effective programs to monitor these vendors. One way to monitor third parties is to require periodic independent assessments of their programs, such as SOC2 reports.

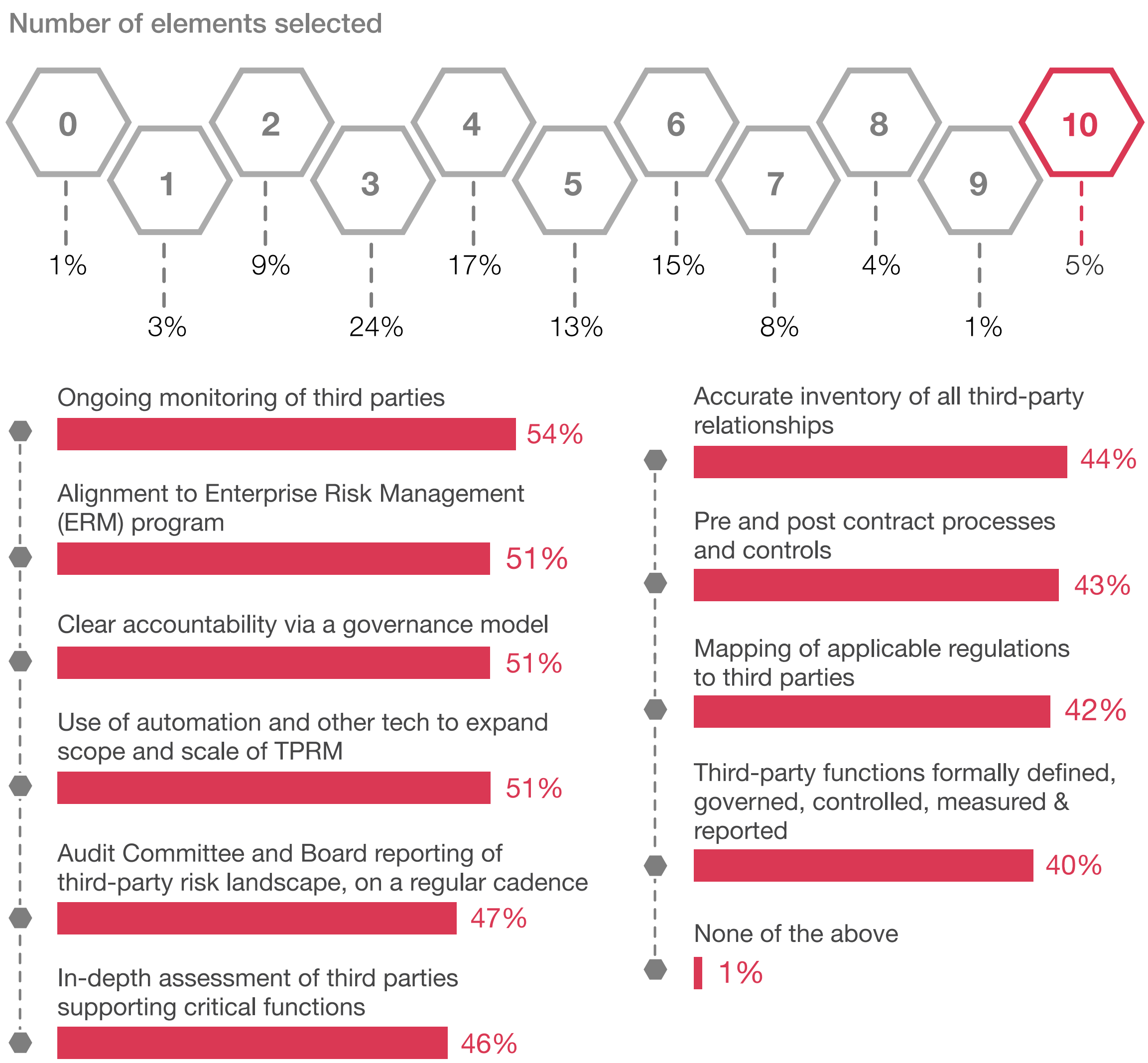
Technology to automate the program

Many organizations are making the investment to automate their third-party risk management processes. Leveraged the right way, technologies can support the onboarding and reporting processes, for example, expediting the assessment process and allowing for more impactful and clearer reporting.

How robust is your organization's third-party risk management program?

Executives surveyed by PwC in early 2021 noted that their companies are relying even more on their third-party risk management program. At the same time, these leaders shared that their organization only had on average about 5 of the 10 elements of a robust program.

As part of the overall dialogue around third-party risk management, directors should ask management how the company's program incorporates these elements. For more information on third-party risk management programs, read **PwC's *Building digital trust: Trust in third parties***.



Source: PwC, *Building digital trust, US Digital Trust Insights Snapshot*, April 2021.

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 longstanding relationships?
- How does management ensure that vendor contracts include language: (1) requiring third parties to comply with applicable territory and company regulations; and (2) requiring third parties to provide independent assurance (e.g., SOC2), including around privacy and security?
- How does management assess risk? Individually? By category? Other?
- How does the company monitor fourth and nth parties?
- How are internal audit and risk management involved in assessing the program?
- How, if at all, does the company receive and review independent assurance reports (e.g., SOC2 reports) to better understand and respond to the privacy and security risks associated with vendors?
- How does management offboard relationships with vendors, including processes to ensure destruction of sensitive data at third parties?

In conclusion

Using third parties is a natural part of business. 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

Maria Castañón Moats
Leader, Governance Insights Center
maria.castanon.moats@pwc.com

Carolyn Holcomb
Leader, Privacy Assurance
carolyn.c.holcomb@pwc.com

T.R. Kane
Principal, Cybersecurity, Privacy & Forensics
t.kane@pwc.com

Dennis Quandt
Partner, Privacy Assurance
dennis.h.quandt@pwc.com

Brian Schwartz
Partner, Risk and Regulatory
brian.schwartz@pwc.com

Dean Spitzer
Principal, Cybersecurity, Privacy & Forensics
dean.v.spitzer@pwc.com

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