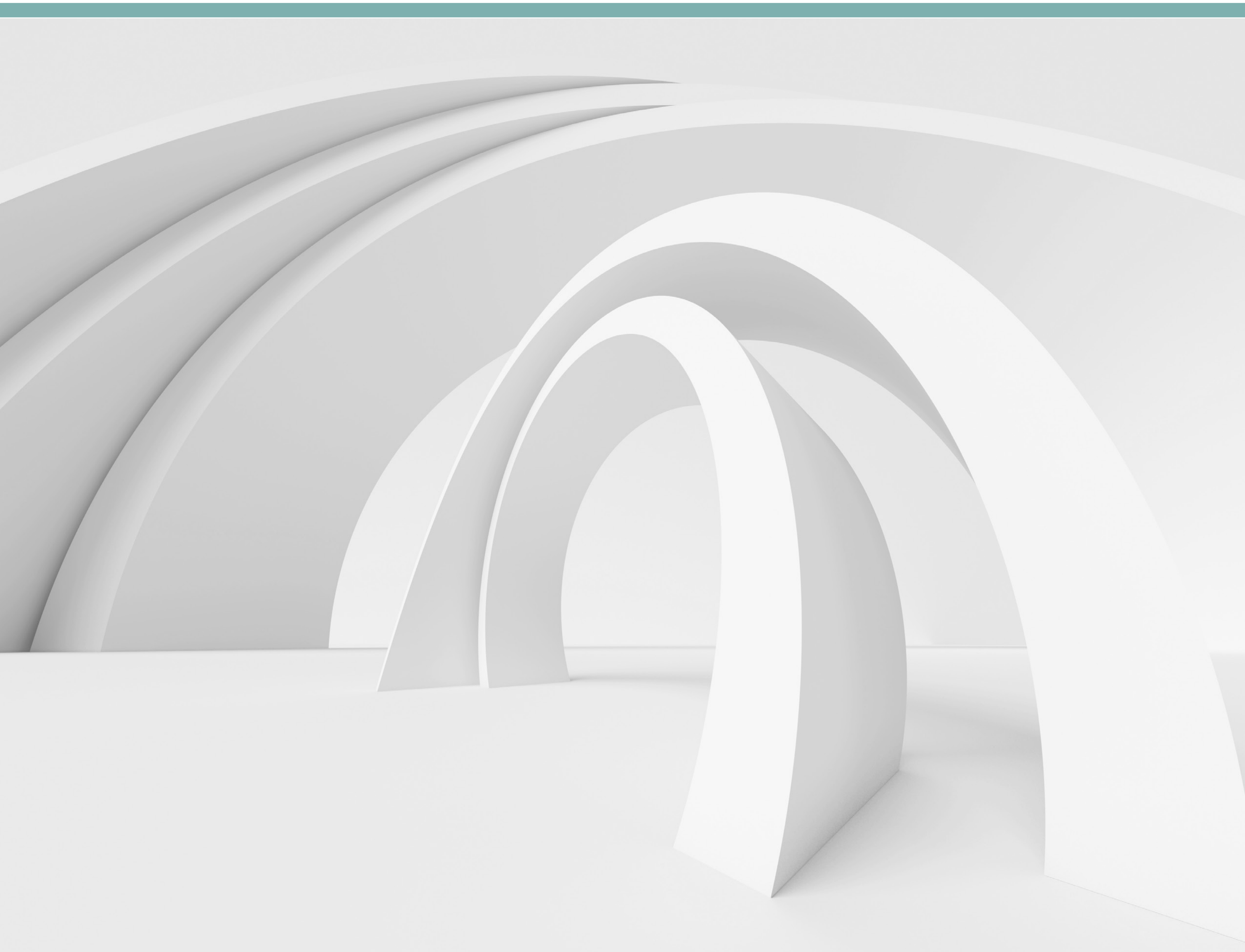
HBR
CONSULTING



A Guide to Developing a Holistic Third-Party Procurement Risk Management Strategy

advisory | managed services | software solutions | insights

The rising importance of managing third-party risk

While third-party suppliers bring many positive opportunities to law firms and other professional services businesses, they also come with risks, given their potential access to firms' and their clients' most sensitive data. In fact, about a third of firms (33 percent) participating in the Procurement Leader Survey, conducted in conjunction HBR Consulting's 2018 Law Firm Procurement Roundtable, had experienced a supplier risk event – such as disruption in a third-party engagement due to SLA/contract breach, information loss, a hacking or security issue, or supplier difficulties with financial viability – in the past 24 months.

Managing third-party risk is more critical today than ever before for several reasons. From increased regulatory pressure to heightened client expectations, firms face new challenges that exacerbate the potential risks suppliers pose.

The top three factors that drive third-party risk are:

- *Regulatory environment:* New regulatory requirements like the General Data Protection Regulation (GDPR) have forced firms to address the management of supplier risk more holistically. According to the Procurement Leader survey, a lack of supplier-related information is firms' top concern regarding GDPR compliance (37 percent).
- *Heightened client expectations:* Clients are increasingly concerned about how firms manage security risks. Clients want to know that their firms are identifying possible third-party supplier risks and taking the necessary steps to monitor and control those risks.
- *Firms' reputations in the marketplace:* Firms have access to some of their clients' most sensitive information, and threats to that information can have a serious negative effect on both existing client relationships and the ability to attract new clients. If a supplier-driven incident were to occur, firms risk hurting their perception not only in the legal industry, but also beyond. Furthermore, the legal industry's security measures in particular are viewed as less sophisticated than other industries, making them a target for hackers.

It is clear that the consequences for firms that fail to manage third-party risk are major. Failure to develop a comprehensive third-party risk management strategy can lead to fines for non-compliance with the GDPR and other data privacy requirements, loss of client revenue, difficulty attracting new clients or potential civil liability. Because of the risks suppliers can pose and the potential side effects they have on a firm's ability to compete, it is critical to develop and execute a third-party risk management program.

> **The top three factors that drive third-party risk are the regulatory environment, heightened client expectations and firms' reputations in the marketplace.**

Three steps to manage third-party risk

According to the Procurement Leader Survey, 53 percent of law firms say they have a formal third-party risk management policy, which is up from 29 percent in 2016. While this growth indicates that firms are making progress toward minimizing risk, about half of law firms are not taking adequate steps to protect themselves from third-party risk.

Gaining complete control over third-party risk can take time, but firms that put a strategy in place now will set themselves up for maximum protection in the long term. Here are three major steps of an effective risk-management strategy.

1. Identify and quantify all suppliers. The first step in managing risk is to identify possible threats. To start, firms should examine all of their third-party relationships in a consistent manner. This includes identifying everything from cloud services suppliers to document management tools to time and billing software. Additionally, firms must identify both IT and non-IT related suppliers – such as HR benefits, staffing support or travel – to get a complete view of their suppliers.

Best practices for uncovering all supplier relationships start with having the right technologies in place. As a baseline capability, firms should invest in a spend visibility system to uncover data on who their suppliers are, how much the firm spends with each supplier and what the relationships look like between different arms of the firm. Traditionally, firms house information about suppliers in disparate systems, which may prohibit them from gaining a full picture of their supplier base. Spend visibility systems centralize all third-party supplier data, making it easier to quickly access and holistically monitor supplier information.

Once firms identify their supplier relationships, they need a systematic approach to evaluate the relative risk of each relationship based on how they engage with the supplier and the supplier's level of access to facilities or systems, along with sensitive firm, employee and client information. Additionally, evaluations should consider the materiality of the relationship, which is a simple measure of how important the supplier is to the firm. Total spend with the supplier, for instance, is a good indicator of materiality.

Ideally, firms will use a standardized, quantitative methodology for measuring risk, such as a scale from 0 to 100, with input from stakeholders engaging the supplier, the suppliers themselves and other functional areas the supplier will work with. Scoring should include attributes such as the degree of access to information, the duration of the relationship or the reputation of the supplier.

Identification of all suppliers is a crucial first step in risk management. Without a complete view of all third parties that interact with the frim, it is impossible to monitor for and prevent risk.

> **Best practices for uncovering all supplier relationships start with having the right technologies in place.**

2. Mitigate the risks suppliers pose. Once firms have identified the relative risk of each supplier relationship, they can mitigate specific risks by addressing them within agreed upon key performance indicators (KPIs) and other contractual agreements for performance measurements. The goal of the mitigation step is to tie a supplier's risk to its contract with the firm, and ultimately stay one step ahead of any possible threats. The KPIs firms establish differ by spend areas, but typically include quality and performance data. The act of monitoring KPIs is itself a measure of risk reduction.

Firms must also ensure they have the correct contractual framework for codifying the obligations and triggers of the relationship, including the right level of indemnification based on the risk factor. Additionally, firms should include the defined KPIs and a monitoring process in the contract they sign with the supplier.

Additional contract terms and conditions – all of which are aimed at mitigating supplier risk – should include:

- Remediation timelines and methodologies for identified security risks
- Breach notifications
- Employee and subcontractor vetting (background checks) and data access rights management policy
- Minimum insurance requirements, including general liability, cyber liability, and errors and omissions
- Patch update notification requirements before technology deployment
- Right to audit clause

While risk will always still exist, the right mitigation approach can help firms prevent as much risk as possible, or minimize the severity of any threats that arise.

3. Monitor ongoing risks. Lastly, firms should establish a supplier relationship management program to constantly monitor the activity of third-party suppliers. While establishing KPIs is a good first step, firms cannot effectively thwart risk without monitoring performance against those KPIs. This step primarily includes reviews and other checks on internal satisfaction and risk.

- *Recurring reviews with suppliers:* Reviews should occur quarterly, and should focus on the performance measures previously agreed to by the supplier. These reviews present an opportunity for firms to conduct audits and security reviews. Key stakeholders should be involved in this process to offer feedback and guidance about supplier performance. Prior to these reviews, firms should track how suppliers are performing against SLAs and KPIs, which will reinforce the expectation that suppliers must demonstrate how they provide value for the firm.
- *Internal satisfaction reviews:* In addition to meeting with the suppliers regularly, firms should also conduct internal satisfaction reviews with those who work directly with the supplier. Many firms use net promoter score to track satisfaction – an index that measures users' willingness to recommend the service to others.
- *Technology capabilities monitoring:* For relationships where suppliers have system access, firms should continuously monitor the supplier's technology capabilities. This step includes preventative testing and spot checks.

If abnormal behavior is found, firms should first discuss with relevant internal stakeholders its severity and the potential plan to address it and prevent future recurrences. From here, based on the response and severity, the issue should be escalated within the firm and with the supplier.

The monitoring phase is an important step in getting ahead of all potential risk. The best way to minimize the effect of third-party risk is by tracking suppliers' performance against pre-defined KPIs, constantly monitoring their engagements with the firm and spotting any issues before they become detrimental to the firm.

Procurement is uniquely positioned to lead firms' third-party risk management

The process of managing third-party risk has historically been decentralized within firms, making it difficult to formulate and execute formal processes. But as the side effects of third-party risks grow, firms need a strategy for implementing and executing this process.

As with any major business endeavor, firms may find that executing a third-party risk management strategy is easier said than done. According to the Procurement Leader Survey, many firms face challenges such as limited resources to manage this responsibility (59 percent) and internal resistance to change (29 percent).

The procurement function can help firms address challenges such as limited resources and internal resistance to change by serving as a trusted partner that can take the lead in identifying, mitigating and monitoring risk. Since the procurement function leads the strategic selection of and negotiation with third-party suppliers, it is uniquely positioned to serve as the central hub for third-party risk management programs.

The best way to minimize the effect of third-party risk is by tracking suppliers' performance against pre-defined KPIs, constantly monitoring their engagements with the firm and spotting any issues before they become detrimental to the firm.

Conclusion

Firms cannot afford to wait for risks to become an issue. It is important to act now and begin following the steps outlined above to create a formal, centralized risk-management program.

As new regulations and changing client expectations continue to increase the risks of third-party suppliers, ensuring your organization is safe from risk can be daunting. Look to HBR Consulting experts with proven industry-specific experience to help you implement a risk management strategy that effectively identifies, mitigates and monitors for the risks suppliers pose. Contact us to learn more about how HBR Consulting can help you implement this strategy.

Connect With An Expert

Lee Garbowitz
Managing Director

O 312.425.4427
E LGarbowitz@hbrconsulting.com