



Register now for your free, tailored, daily legal newsfeed service.

Questions? Please contact customerservices@lexology.com

[Register](#)

Why Third-Party Risk Management Matters in Compliance

Global | November 16 2020

What does third-party mean? Whom does it cover?

Existential philosopher Jean-Paul Sartre's famous quote "*L'enfer, c'est les autres*" can be translated as "hell is other people". In a global economy working with third parties is a matter of reality and, if not managed properly, their transactions can create hell. In order to understand third-party risk management, we should first concentrate on the definitions.

In Anglo-Saxon law, the term "third-party" means real and legal persons representing a company in a business relationship and legally binding that company with its transactions on behalf of the company. Generally, the company is the "first party", the customer and employees can be deemed as "second party", and the providers of products and/or services, such as suppliers, consultants or intermediaries, that help the parent company achieve its sales, marketing and company goals are described as "third-parties".

Unlike the concept of "well-intentioned third-person", which we frequently apply in Turkish law, the broadly-defined term third-party mentioned in Anglo-Saxon law, refers to any natural and legal person such as suppliers, business partners, distributors, agents, and consultants who provide goods or services to the company. In the event of any illegality arising from third-party faults during activities carried out on behalf of a company, the legal liability of the "first party" company arises, as well as that of the relevant third-party. As the ratio of third-parties a company engages with grows significantly, so do the risks they pose.

What are the potential risks associated with third-party relationship?

All actions in the business world carry their own risks. In risk management reducing risk to zero can mean not doing any business at all, so we should be realistic. That is precisely why companies should rank their risks, focus on the correct red flags, and spend their time and investment to manage high-risk areas. While there are some commensurable and controllable risks, there are also jeopardous ones that can cause irreversible damage, exposing companies to financial loss, non-compliance, regulatory action, litigation, loss of customers and clients, and reputational damage.

It should be emphasized that whether a third-party relationship poses a high-risk, and the underlying reason for a third-party's involvement, are different in every company. There are a number of factors that affect the former, such as the field of a company's activities, the business field of a potential third-party, and the subject and scope of a potential third-party relationship, which might be outsourcing services, supplying products, granting agency, or entering into new business partnerships, among many other reasons.

Feedback



Are your business activities regulated? Is your company 100% domestic or do you have foreign affiliates? What is the scope of activity to be conducted with a potential third-party? What is the estimated degree of a third-party's involvement in your company organization and their level of access to your business data? Will you have direct control and close oversight on a third-party's activities or is it an engagement for your offshore subsidiaries with limited remote monitoring? To what extent can a third-party affect your company's business activities and customer relationships? These are just a few questions to urge you to raise your awareness, and they're just the tip of the iceberg.

What are the fundamental steps of effective third-party risk management?

The first requirement is for your company to be familiar with the nature of risk management plans. The main goal here is not to reduce the use of third-parties but, as mentioned above, it is to use third-parties effectively for your company's best interests by identifying, assessing and managing the risks associated with third-party relationships.

It is crucial to be aware that risk management is not a "tick-box" program to be applied all at once. It is an ongoing process that enables you to assess, control and oversee your third-party relationships from before they start, right to the finish. Therefore, assessing your company's current organization to ensure you have the capability to handle such third-party relationships matters, because every third-party engagement requires ongoing oversight, periodic auditing, control and, when required, intervention. Consequently, entering into a relationship with a third-party is a decision that should only be made once you have assessed both your own company and the third-party.

Even though the implementation of third-party risk management programs will vary depending on the scope of a relationship, the following points are the backbone of any third-party risk management process, and will undoubtedly apply:

1. Risk Assessment
2. Due Diligence
3. Comprehensive and Risk-Based Contract Structuring
4. Ongoing Oversight and Control

Risk assessment is the cornerstone of a strong risk management program, that should include the following steps:

- i. deciding whether or not to include a third-party for a particular purpose, identifying the business rationale lying behind involving a third-party in a transaction, understanding the reason for using a third-party instead of inhouse procurement, and explicitly representing the prior with its financial, legal, operational and strategic results by comparative risk/reward-based analysis
- ii. identifying and assessing the potential risks and vulnerabilities associated with involving a third-party by taking into consideration the subject and scope of a relationship 
- iii. comparing potential third-parties and assessing their qualifications, their compliance with your company's business strategies, and their ability to respond to your company's expectations
- iv. defining the risks associated with a third-party under consideration, assessing their proficiency and adequacy for a potential transaction, and representing why engaging with them is in your company's best interests for long-term success.

Throughout the process, risk assessment should be conducted in a comprehensive and transparent manner by your company's authorized body, and in compliance with your company's codes of conduct, compliance policies and procedures.

The next step in effective third-party risk management is a comprehensive due diligence program designed to provide you with all the required information about a potential third-party. The program should focus on a third-party's financial condition, their business operations, qualifications and experience, their compliance with regulations, litigation status, and reputation. An effective due diligence program not only illustrates all the associated risks, it will also help you to rank your risks allowing you to focus on the highest-level ones. It should be kept in mind that the extent of any due diligence depends on the nature and size of the proposed relationship. This is why due diligence programs, as well as the contracts, should have a risk-based structure.

However, circumstances may sometimes dictate the need to take unexpectedly quick decisions. "Great haste makes great waste", they say, but it does not have to be like that. Even when conditions are not suitable for your company to conduct enhanced due diligence and there is pressure to sign a contract for a third-party engagement, you should consider "post-contract due diligence". It is possible to conduct due diligence after establishing a third-party relationship to assess whether it is in your company's best interest to involve the third-party in a transaction. However, you should ensure that you have the right to terminate a relationship, in the event that your risk / reward balance gives you a red flag in a post-contract due diligence report. Providing a mechanism for "restoration" is also possible with creative contract drafting.

Pre-contract or post-contract, in either case, it is not possible for your company to benefit from due diligence to the fullest extent if you are not provided with a strong and creative contract responding to your business concerns. Contract drafting is a crucial part of risk management programs because it is where the process of identifying and assessing your risks progresses to taking precise actions. Therefore, your contracts should be tailor-made and respond to your company's concerns, meet your company's financial and operational expectations, and the business aims of entering into a third-party relationship. You should ensure that your contract provides your company with an adequate level of protection and indemnification. If you would like to have a deeper insight on contract drafting and get some tips about essential clauses, please see our article [**5 Contract Clauses to Mitigate Third-Party Risks**](#).

As previously mentioned, risk management is an ongoing process. Your company is responsible for controlling and monitoring third-party relationships. It is a responsibility that remains until the termination of a relationship, and even beyond that, sometimes if there are any post-termination liabilities. You should ensure that the risk /reward balance, ranked-risk and a third-party's compliance remain the same as reflected in your due-diligence report during the relationship. Additionally, assessing whether a third-party fulfils its contractual obligations and complies with applicable regulations and your company's compliance program can quickly help to identify whether a third-party relationship harms your business operations. Therefore, your company should have an authorized body dedicated to monitoring and auditing third-parties and reporting suspicious circumstances that may pose a risk to your company

Feedback

Conclusion

Most companies attach high importance to due diligence programs, however they constitute only a part of risk management plans. Third-party risk management plans are an ongoing process that start with the decision to involve a third-party in a transaction; they proceed with identifying and assessing your risks, providing protection and monitoring the relationship, which could change your assessment results at any time. The underlying rationale of a

risk management plan is always to provide your company with the necessary information, awareness and the fullest level of control over your company's third-party relationships. To conclude with a quote from another great philosopher Thomas Reid, "*a chain is as strong as its weakest link.*"

CBC Law - Altug Ozgun and Burcu Seven

Powered by

LEXOLOGY.

Feedback

