REFINITIV EXPERT TALK

MANAGING THE BUSINESS AND LEGAL RISKS OF WORKING WITH THIRD PARTIES

In the eyes of the law, third parties – suppliers, distributors and other business partners – are considered an extension of your company, so it's in your company's best interest to build third-party due diligence in your compliance program.

Right now, every business story is a COVID-19 story; the pandemic has called into question business models from higher education to healthcare (do we ever need to go to the doctor's office again for routine things, or will telehealth suffice?) and has disrupted day-to-day business operations.

Business travel has largely ceased, and entire countries remain closed to travelers. Suppliers have temporarily shut down, and companies are casting about for alternative supply chains, while the pandemic-related high demand for some categories (ventilators and other respiratory equipment, for example) has companies and providers looking to new sources to augment supplies.

Some companies serving healthcare segments where there is currently little demand (elective orthopedic procedures, for example) are temporarily switching their manufacturing operations in order to provide items vital to pandemic patients. This all represents rapid change and new kinds of risks.

No matter what size a company is, chances are that it is engaging with some third-party partners such as business consultants, distributors, sales agents, customs agents, contractors or others. Ethically and legally, organizations are held responsible for the compliance of third-party partners as an extension of the company that has hired them.

Even without the threat of headline-rocking scandals, as part of your supply chain, third parties can significantly jeopardize your business and interests – and potentially the healthcare system, or worse, patient lives.

In fact, in the past three decades, most of the high-profile corruption cases in which life sciences corporations faced serious indictment charges – and hundreds of millions, even billions of dollars in fines and penalties – involved third parties that performed the majority of the wrongdoing. (Editor's note: To name only one example among many, perhaps the most significant in the healthcare space, third parties acting on behalf of Siemens around the world were involved in paying bribes and inflating prices. Siemens was prosecuted under the FCPA and paid more than $1.6 billion in fines, penalties and disgorgement of profits).

Whether your entire team is unaware of the unethical practices of third parties, or someone internally is directing them, your management and executive team will be held accountable for their transgressions.

Keeping pace with a changing risk profile

During these pandemic times, and indeed, following any type of disaster (the global financial crisis of 2008 or Hurricane Katrina, for example) there is an increased risk of fraud and corruption. Many third-party providers of services or goods are, at present, closed and entire marketing regions are shut down. This creates pressures on many companies trying to maintain their core businesses by accessing new supply chains and distribution networks. Many will shift their focus, temporarily, to products with direct relevance to the pandemic, and this will cause them to work with new suppliers.

As companies turn to third parties with whom they have not previously engaged, it is important to have a process to both vet and monitor them to make sure they don't have a history of bribing government officials that hold the power over necessary approvals or those that have purchasing authority at hospitals. They must be investigated to make sure they don't engage in the practice of buying brand-name parts from your company and mixing them with cheaper parts of others, in order to maximize profits, and other corrupt practices.

Below, we outline the best practices and key considerations for creating and managing a third-party due diligence program.

Frameworks for due diligence

Locally, regionally and globally, standards and regulations are established, designed and rigorously enforced to protect consumers and the environment, as well as to promote fair competition among businesses, among other positive factors. The principles of "The Seven Elements of an Effective Compliance Program" under the framework established by the U.S. Office of the Inspector General are generally accepted and adopted globally to help guide companies in day-to-day operations, while aligning with global laws, regional codes and industry best practices. These standards include "any representative of the company (i.e., agents, distributors, contractors, etc.) with regard to the compliance program, code of conduct/ethics, corrective action plans, etc."

In addition, the U.S. Department of Justice (DOJ), Criminal Division, Fraud Section, builds on these elements using the industry-agnostic "Evaluation of Corporate Compliance Programs" guidelines, which were updated and expanded in June 2020, and are also generally accepted globally. These guidelines contain three fundamental questions, including 12 topics or elements, organized around what prosecutors should assess to determine the effectiveness of a compliance program and how that translates into penalties and fines.

Organizations are responsible for the compliance of third-party partners, as they represent the company, and therefore must perform appropriate compliance due diligence and monitoring during contracting. That means companies must decide which policies and procedures their third-party partners will follow, train them through main policy procedures and ensure that risk is minimized as much as possible.

Best practices for third-party due diligence

While no one-sixe-fits-all third-party due diligence program exists, a "right-sized" approach to third-party due diligence at the highest level comprises three core elements:

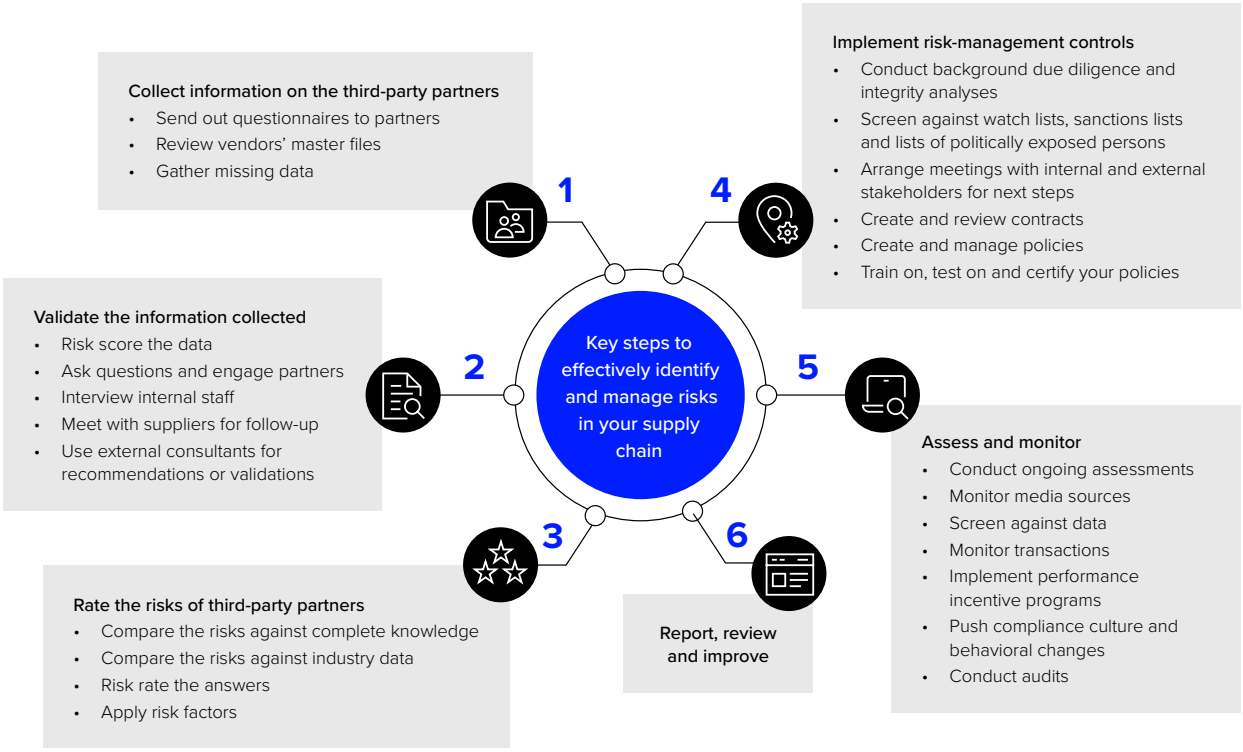
1. Collecting information on both potential and existing third parties
2. Conducting a risk-based analysis to validate information collected while identifying and rating any potential risks
3. Coming to an objective and defensible conclusion on whether or not to do (or to continue to do) business with them (see Fig 1)

The due diligence program will help ensure that appropriate review of each third party takes place so you can understand any associated risks, decide whether to move forward with each partner and put control factors in to place to control and mitigate potential and existing risks.

Kicking off a compliance program with an objective risk assessment helps you create a proactive, preventative program. By helping uncover and rank current and potential risks with regard to third parties, a risk assessment will inform how to structure your third-party due diligence program, or, if you already have one in place, how it should be tailored and customized based on your organization.

Figure 1

Key steps to identifying and managing risks in your supply chain



As you begin structuring your third-party due diligence program, create an inventory of all your vendors that work for you. Then, establish how to classify them – meaning are they suppliers, channel partners, healthcare providers, etc., – so you can rate the level of potential risk they might carry for your organization, and prioritize those you most need to screen.

For example, the landscape vendor likely poses a much lower compliance risk to your organization than the distributor selling your medical technology or pharmaceutical products to a government hospital. It is often helpful to start with a facilitated roundtable to convene members of the procurement, business, legal, finance, risk and compliance teams, to review and discuss the third-party partner categories across the company.

In addition, determine if you have too few or too many third-party partners to meet your business needs, because, if and where possible, winnowing the field has the twofold benefit of streamlining compliance risks and saving management time and resources.

As part of this step, you should determine the process for adding new third parties. For example, answer questions like:

- What is the business rationale for adding them?
- Who is in charge of gatekeeping the selection and onboarding process?
- How will new vendors be vetted and what will the contract say?
- What training will be provided?

It is critical that all third-party partners understand and agree to practice appropriate due diligence practices, which involves consenting to answering questions, undergoing background checks and providing relevant documentation, as requested and agreed upon.

Contract considerations

To mitigate risk and remove personal bias from the process, it is best to have a standard third-party contract and model provisions for the different risk levels. This will help safeguard against third-party partners who technically do not qualify based on your due diligence program from, say, becoming admitted through personal connections or grandfathered in despite new policies.

Furthermore, contracts should contain a “right to audit” clause – and a process for regular auditing and monitoring, even without advanced notice, to ferret out any discrepancies or changes. For example, a third-party partner requests commissions to be paid into a different bank account after securing your significant contract, and the new bank account is used to distribute improper payments, putting your company at risk. Or your third-party distributor hires a sub-distributor with a history of misconduct unbeknownst to your company, yet the liability of your company remains, even through the myriad layers by which your products are sold.

The standard contract should also outline how subcontractors will be identified, risk-ranked, tiered and handled. In some countries, it is not permissible to interfere with the relationship between your contracted partner and its subcontractors, but at least you have the right to be informed about who is ultimately acting on your behalf. In addition, the contract should outline services, compensation, payment terms and termination stipulations.

Implementing your due diligence program

With your program structured and standard contracts in place, you can then begin implmenting your program. The question is, who at your company will be conducting due diligence and how? What questions will be asked? How will the responses be validated?

For reference, the DOJ offers a list of 119 questions in its guidelines that regulators may ask in the case of alleged misconduct. You will want to design your program to be sure you will be able to answer relevant questions about your third parties. Officials will be looking to see how your company’s third-party management process corresponds to the nature and level of enterprise risk identified, and will be seeking evidential documentation, such as the initial questionnaire, approvals, independent verification through due

diligence, documentation, certification, on-site audits, interviews, training, processes, risk scores, etc.

As you gather background, you want to be as certain as possible that the third party provides accurate information and is not somehow incentivized, such as by an inflated commission-based pay scale to alter the answers to win the account. Leveraging the expertise of an outside agency to conduct the due diligence and research can be helpful in driving objectivity into the risk assessment, program creation and implementation.

Your due diligence program should prioritize the most vulnerable third-party areas of compliance and create a risk-scoring methodology on which to base the diligence. For example, what types of risks are considered – geography, industry sector, transactional (licensing and permits), government involvement and/or politically exposed persons, volume of spend, etc. From there, you will need to outline how risks will be identified, reviewed and resolved.

The onboarding process

Onboarding vendors is another key consideration, especially considering that most companies have budget constraints. This is another way risk-scoring your third parties can be helpful, as it will help you prioritize and align training procedures according to potential risk.

As with the example above, while some companies drive a hard line and require all third parties to complete due diligence training, there are some cases in which, say, the contract manufacturing partner that provides the product versus a high-volume supplier that provides the packaging, might not be given the same level of rigorous training as the manufacturing team developing your medical devices or pharmaceuticals.

For reference, compliance onboarding software is available that incorporates and accommodates the recommended best practice elements. These software platforms help streamline the onboarding process and improve data collection and record keeping by enabling dashboards, reporting tools, automation, approval workflows, built-in risk scoring and analysis, as well as robust audit trails, among other features.

Continuous monitoring

Knowing an initial third-party screening process and due diligence program cannot protect a company from all risks, mechanisms should be put in place to regularly monitor and assess the compliance of third parties. So, as part of your program's structure, you need to build in rescreening, including criteria for frequency, documentation and record keeping.

You also need to outline how uncovered issues will be handled and resolved while accounting for internal review and resolution, timely voluntary disclosure and cooperation with any outside investigation. While your due diligence may be robust, it is only valid at the point in time it was conducted, which further supports the need for continuous monitoring.

A proactive culture of compliance

In the real world, internal politics, inherent biases, and personal agendas often impede an organization's ability to conduct due diligence and make rational fact-based decisions about third-party partners. That's why it is critical to create a proactive culture of compliance in which all employees and third parties are held responsible and accountable for due diligence. Keep in mind, the business is ultimately responsible for its third parties, not the compliance function.

The message needs to come from and be role-modeled from the top, middle, down and across the organization, while allowing for and being sensitive to regional and geographic differences. Many companies also find it beneficial to enlist external, experienced compliance specialists to help objectively mitigate risks, while helping align corporate teams and institutionalizing a compliance culture and program.

Again, there is no one-size-fits-all solution. Each company needs to deploy the compliance program that's right-sized based on its specific needs. Certainly, navigating the third-party due diligence can be daunting, but it's far better to do the hard work up-front, than to find out you've put your business – or patients – at risk.

Original article first published on MyStrategist.com, June 2020.

Authors:

J. Mark Farrar is a partner and the global practice leader of the Life Sciences Governance, Risk Management and Compliance practice at Guidehouse.

Thomas K. Hauser is an international practice leader for the Life Sciences Governance, Risk Management and Compliance practice at Guidehouse.

Juliet Lui is the former Director of Corporate Strategy & Development of The Red Flag Group.