POLICY & MEDICINE
COMPLIANCE UPDATE
Reprinted from
Volume 10.1 | January 2024

FEATURE

All Parties Are Not Created Equal

Managing High-Risk Third Parties

By Mark Pearson, Dimple Thomas, and Paul Silver[1]

Summary: Bribery and corruption are among the most prevalent issues that result in regulatory scrutiny, enforcement actions, and reputational damage. Therefore, having a specific, tailored, and well-documented Third-Party Due Diligence program focusing on Anti-Bribery/Anticorruption issues, overseen by the corporate compliance function, is becoming increasingly common. This article applies to those organizations looking to establish an ABAC TPDD program for the first time and those wishing to refresh their approach.

Many organizations that operate in the pharmaceutical and medical technology sectors often find out too late that some of the third parties with which they do business may represent a direct and costly risk to their own business. These third-party risks should not be overlooked, as they can have wide-ranging and long-lasting negative effects upon companies, including but not limited to (i) damaging the company's reputation in the marketplace, leading to loss of owner or shareholder value, (ii) causing non-compliance with relevant regulations or laws, (iii) being subjected to enforcement actions and related legal costs, or (iv) perhaps even causing negative impacts on patient safety, which the Office of Inspector General for the Department of Health and Human Services ("HHS-OIG") highlights in its new General Compliance Program Guidance[2].

The Goal

Chief Ethics & Compliance Officers ("CCOs") are likely familiar with the prevalence of issues concerning the third parties their organization does business with across the world, especially with the increase in country-specific laws, compliance regulations, and standards. Regulatory bodies across the globe now expect organizations to not only be compliant with laws and regulations but also to engage in ethical and responsible business practices, especially when it comes to managing their third-party relationships. In 2023, the U.S. Department of Justice ("DOJ") updated its guidance on evaluating corporate compliance programs.[3] These updates emphasized a number of aspects related to third parties, such as the need for companies to take a more holistic view across their third-party lifecycle and the need to apply a risk-based approach to due diligence on its third-party relationships.

Bribery and corruption are among the most prevalent issues that result in regulatory scrutiny, enforcement actions, and reputational damage. It is also commonly understood that these terms can have different definitions and cultural connotations depending on where companies operate. These issues may arise across a number of processes and functional areas that include, but are not limited to, procurement and supply chain, R&D and quality assurance/approvals, marketing programs, health & safety initiatives, and government tenders/bids. Regulators are increasingly concerned with not just bribery of government officials but also general commercial bribery, kickbacks, and conflict of interest.

In many organizations, these issues fall into the domain of the CCO. Therefore, having a specific, tailored, and well-documented Third-Party Due Diligence ("TPDD") program focusing on Anti-Bribery/Anticorruption ("ABAC") issues, overseen by the corporate compliance function, is becoming increasingly common.[4] Furthermore, continuous enhancement of the ABAC TPDD program can help any TPDD program stay relevant and effective over time.

This article applies to a broad audience of CCOs and organizations, including those organizations looking to establish an ABAC TPDD program for the first time and those wishing to refresh their approach so that the program remains relevant to the specific environments and circumstances facing their organizations.

Avoiding potential bribery and corruption situations is the paramount goal of any ABAC TPDD program. Doing so requires a demonstration that the organization has thoughtfully considered the creation of specific ABAC TPDD procedures relevant and effective. For example, a primary objective of the program should be identifying the high-risk third parties that pose the greatest risk to the organization.

To achieve this objective, we outline a basic 3-step framework that can help identify which third parties represent the highest risk to an organization and provide a foundational starting point for the organization's robust third-party risk program.

Step 1: Identify and categorize all third parties with whom the organization does business with.

Step 2: Determine the categories and attributes of third parties that represents the highest relative risk.

Step 3: Provide an overview of some basic third-party due diligence ("TPDD") procedures.

Step 1: Identifying and Categorizing All Third Parties

Upon first thought, identifying all the third parties an organization does business with may seem like an easy task. However, many organizations quickly learn that there can be various unforeseen complications to this task, such as the existence of multiple overlapping, conflicting, or simply out-of-date data sources that need to be considered.

It is important to focus on capturing the majority of third parties in a reasonable timeframe and with reasonable effort rather than striving for absolute perfection in identifying every single third party. The strive for perfection in identifying all third parties can become an unachievable goal that consumes an organization's time and resources. Also, any third parties not initially identified and categorized can be added at a later date. An achievable goal for most organizations is to aggregate a single listing of active third parties from the vendor master(s). An additional step might be to disseminate a tailored survey to the organization's procurement/supply chain/distribution ecosystem.

A common pitfall to avoid when identifying all third parties is to combine this exercise with other third-party initiatives or activities (for example, a third-party "rationalization" if there are more than one vendor masters/sources of record). Having clearly defined goals for this exercise can help prevent this from becoming overly and unnecessarily complicated.

Once a single listing of an organization's third parties has been compiled, the process of risk-based categorization can begin. The goal of this categorization is to separate the various types of third parties by their perceived risk to the organization. A basic categorization scheme could include the type of service or the nature of the product provided by the specific third party (e.g., distributors/resellers, direct and indirect materials vendors, etc.).

Step 2: Determine the Highest-Risk Category of Third Parties

Many organizations have hundreds if not thousands of third-party relationships across a wide range of activities such as supply chains, sales, and other ancillary process. A risk-based approach of categorizing third parties can keep costs reasonable while helping focus the more intensive procedures on the higher risk categories. Consequently, there cannot be a one-size-fits-all approach to TPDD procedures.

TPDD procedures for third parties should be tailored to assess individual business practices, reputation, financial stability, and legal and ethical compliance, such that they are proportionate to the risks presented by each third party. Thus, a categorization exercise is essential to determining the population of third parties that likely represent the highest risk to the organization.

Having categorized third parties into the broad buckets listed above (e.g., distributors, direct materials vendors,

etc.) is only the beginning. There are diverse sets of characteristics unique to third parties within each of those broad categories. It is, therefore, important to take the next step to identify and define specific risk characteristics or activities of the third parties for further subdivision. An example of this would be a distributor who does not sell the organization's product to government customers versus one who does or one who represents the organization in promotional events or interactions with Health Care Professionals ("HCPs").

The type and number of sub-categorizations typically depend upon factors that are unique to the organization, such as the sales process (e.g., sales agents, distributors, or resellers), the business growth strategy (e.g., increasing investment in emerging markets, new product indications, etc.). When determining what risks should be considered, it is advised to seek input from functions that interact with third parties, such as procurement, internal audit, legal, and accounts payable (see Figure 1 below for a generic illustrative example of potential risk characteristics).

Every organization has its own specific risk tolerance, and therefore, it is important to understand that each organization's highest risks may be different from other organizations. If possible, define and consider any activities or characteristics of this highest-risk category to further narrow this sub-population. The importance of this exercise is tailoring this sub-population to the specific organization and its risks.

Adequately documenting the risk ranking approach is of paramount importance when considering the TPDD program's auditability and defensibility. Many organizations have general risk ranking policies (i.e., reperform due diligence every three years) that appear sound but lack a documented, supporting rationale. Additionally, documenting the risk ranking approach helps increase the continuity of the TPDD program; too often, we see risk ranking criteria live in the mind of its creator, as opposed to formal documentation. Documenting the rationale of the organization's risk ranking approach prevents the likelihood of this information becoming untraceable or missing when certain employees leave the organization.

The risk ranking approach should be defensible to regulators, who will not only want to understand the policies in place but the rationale behind them and how the organization believes they significantly mitigate or address third-party risk. This includes demonstrating the rationale for the allocation of resources to these mitigation measures. This includes aspects such as (i) a team that is adequately resourced with the required skillsets, has cross-functional representation, and the right level of oversight and autonomy, (ii) investments in

FIGURE 1: *Example of Basic Risk Categorization*

Characteristics (illustrative examples)	High	Medium	Low
Annual volume of business	>$10m	$5-10m	<$5m
Government Customers / tenders	Yes	Indirectly	No
Involvement in HCP interactions	High	Low to Medium	No
Contract Complexity	High	Medium	Low
Contract Type	Cost Plus	Hybrid	Fixed Fee
Relationship Origin	Sole-Sourced	Hybrid	Competitive Bid
Historical Relationship (qualitative)	Poor	Neutral	Trusted Advisor
Data Analytics Results / Issues	Many exceptions	Some Exceptions	Few Exceptions
Audit rights	None-Weak	Standard	Strong

policies, processes, and methodologies, and (iii) investments in technology, especially analytical solutions, provides access to real-time TPDD and compliance data that is accurate and timely and has the ability for continuous improvements through feedback loops.

In our experience, regulators are NOT looking for perfection; rather, they are looking for documentation supporting an intentional and defensible rationale for the TPDD procedures undertaken.

For organizations operating in the pharmaceutical and medical technology sectors, third-party distributors, marketing firms, and liaison agents operating in foreign markets are examples of third parties that represent their highest risk category.

An illustrative set of characteristics or attributes that may be considered in the risk ranking of third parties is shown above (Figure 1). Each third party is assigned a risk score (high, medium, low, or something similar) across each of the characteristics based on the applicability/extent that it applies to the organization. A cumulative score (typically, a weighted score) is then derived for the third party, which in turn determines the overall risk tier of the third party. As an example, a sole-sourced distributor in China that handles government customers would typically fall in the "high" risk tier, as opposed to a law firm in the US or Canada that handles employee taxation matters that would typically fall in the "low" risk tier.

Step 3: Overview of the Design of ABAC TPDD Procedures

Describing a comprehensive set of procedures that an organization may want to consider for its ABAC TPDD is beyond the scope of this article, as any procedures included in the program must be relevant and tailored to the organization. A key component of any ABAC TPDD is the ability to demonstrate considerate thought and attention went into tailoring the ABAC TPDD to the business context and nuances of that organization.

While approaches to an ABAC TPDD program may vary, there tends to be some commonalities, such as subjecting the third parties to differentiated levels of procedures, based on their risk tiers (Figure 2).

As can be seen in Figure 2, Tier 1 third parties represent those evaluated as the lowest risk. Some typical procedures for this group may involve findings of interest pertaining to corporate registration information, identification of directors, material litigation or adverse media identified, classification as a State-Owned Entity or politically exposed persons (PEP), sanctions, and watch list screening.

For categorized entities that have been evaluated as medium (Tier 2) or high (Tier 3) risk, additional ABAC TPDD procedures may be warranted. For example, some of the additional procedures applied to Tier 2 might include findings related to the identification of shareholders, bankruptcy searches or other tax concerns; public records searches on key third-party personnel, and the results of reference checks.

For the third parties that have been evaluated as Tier 3, more intensive adverse social media searches or targeted interviews can be conducted with key third-party personnel regarding the factors or findings that have led them to be evaluated as the highest risk to the organization.

Conclusion

CCOs are increasingly becoming aware of the heightened regulatory attention around the risk related to third parties and investing in building/enhancing TPDD

FIGURE 2: *Third Party Risk Tiers*

programs that enable their organizations to identify the high-risk third parties that pose the greatest risk and remediate those risks in an effective manner. Beyond treating this as a cost of compliance, CCOs are now looking at this as a sound measure that can help avoid unexpected adverse developments like regulatory inquiries or enforcement actions in the future.

As mentioned at the beginning of this article, we have written this to apply to a wide audience of CCOs and their organizations – from those organizations with no ABAC TPDD program in place to those organizations that have programs but may want to refresh their approach to help their program remain relevant to their ABAC TPDD goals and the specific environment and circumstances facing their organization. We provided a basic 3-step framework that can help identify which third parties likely represent the highest risk to an organization and provide a foundational starting point for any robust ABAC TPDD program.

In conclusion, having some form of ABAC TPDD procedures performed on the highest-risk third parties is strongly recommended. Having those ABAC TPDD procedures well-documented within a broad ABAC program can provide a foundation for future enhancements and revisions as the organization's environment, marketplace, strategy, or other factors change. This is a critical topic for organizations operating in the pharmaceutical or medical technology sectors, especially those that conduct business in multiple countries.

Mature organizations are now investing in technologies like artificial intelligence and machine learning into the risk categorization and due diligence processes allow for faster and more real-time access to insights, leading to faster responses and remediation of any identified issues. Automation of the basic screening processes for the lower risk third parties also helps reduce the associated effort and costs, freeing up resources to perform more targeted audits and transactional reviews for higher risk third parties. Tech-enabled programs also allow for continuous enhancements through feedback loops, which helps the program stay relevant and effective over time.

References

1 Mr. Pearson is a Principal with Deloitte Financial Advisory Services LLP. Ms. Thomas is a Deloitte Financial Advisory Services India Private Limited Managing Director. Mr. Silver is a Principal with Deloitte & Touche LLP.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services, and its affiliates. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2024 Deloitte Development LLC. All rights reserved.

2 *See* U.S. Department of Health & Human Servs., Off. of Inspector Gen'l, *General Compliance Program Guidance*, 76 (Nov. 6, 2023), https://oig.hhs.gov/compliance/general-compliance-program-guidance/.

3 *See* U.S. Department of JUStice, crim. Div., evalUation of Corporate compliance programS (updated Mar. 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

4 As used in this article, ABAC refers to both domestic (U.S.) and international bribery and corruption.

To learn more about Deloitte's Third Party Diligence Support for the life sciences industry, contact:

Mark Pearson
marpearson@deloitte.com

Paul Silver
psilver@deloitte.com

Dimple Thomas
dimthomas@deloitte.com