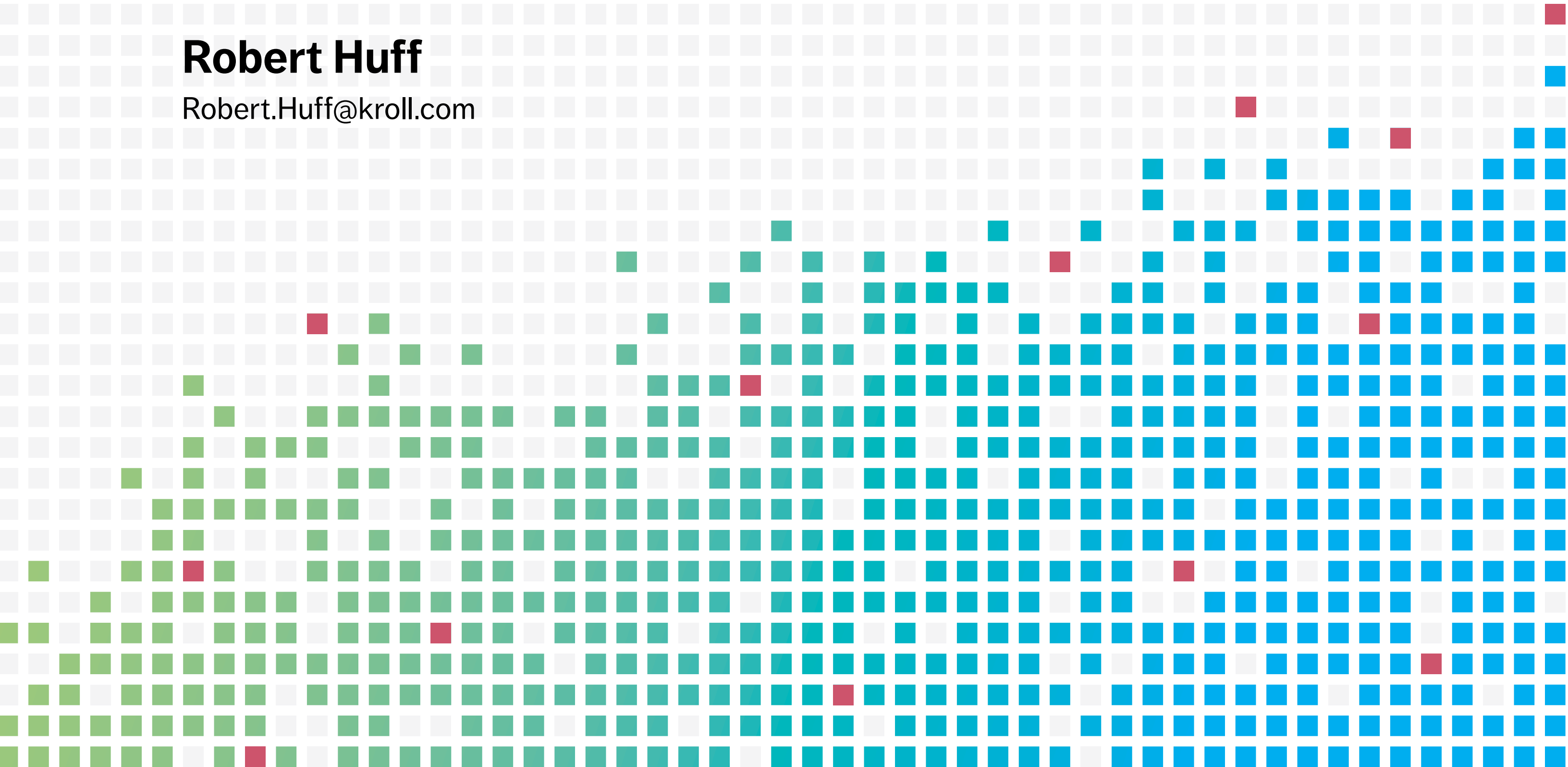
ONGOING MONITORING OF THIRD PARTY RELATIONSHIPS

Defining a risk-based, scalable, and sustainable approach

Robert Huff
Robert.Huff@kroll.com



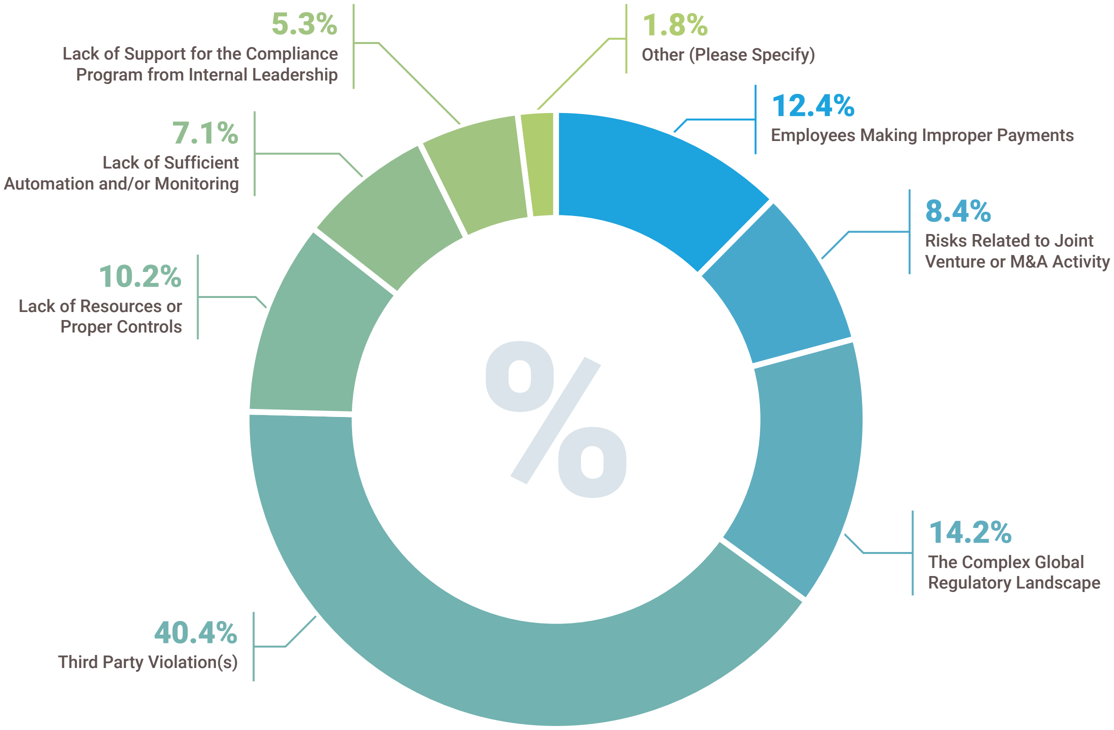
Statements herein concerning financial, regulatory or legal matters should be understood to be general observations based solely on Kroll's experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which Kroll is not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas.

INTRODUCTION

As companies continue to globalize their business opportunities, they are exposed to an ever-widening environment of anti-bribery and anti-corruption regulations. Moreover, the enforcement of such laws is increasing; for example, 2016 was a record year in terms of the number of Foreign Corrupt Practices Act (FCPA) actions brought by U.S. regulators and the amount of monetary penalties imposed.[1]

While many risks can compromise an organization's compliance with anti-bribery and anti-corruption regulations, third party relationships are especially problematic. In fact, third party violations were cited as the top risk to their organizations' anti-bribery and anti-corruption programs by 40 percent of survey respondents in the "Anti-Bribery and Corruption Benchmarking Report – 2017" (ABC Report), published by Kroll and the Ethisphere Institute.[2]

Q: What Do You Perceive to Be the Top Risk to Your Anti-Corruption Program in 2017?



While there is little disagreement on the importance that regulators attach to conducting due diligence prior to onboarding a third party, there is much less clarity and consistency in terms of what should be done post-onboarding. Once a third party passes an organization's initial vetting process, what are the expectations and options in terms of ongoing monitoring to detect changes in the bribery and corruption risk they pose?

[1] F. Joseph Warin, "2016 Year-End FCPA Update," Harvard Law School Forum on Corporate Governance and Financial Regulation, Jan. 19, 2017, https://corpgov.law.harvard.edu/2017/01/19/2016-year-end-fcpa-update/.

[2] "Anti-Bribery and Corruption Benchmarking Report - 2017," Kroll and the Ethisphere Institute, https://goo.gl/CS3i3J.

SECTION ONE

REGULATORY GUIDANCE

Regulators of the FCPA and similar anti-corruption laws have been consistent in their messaging that third parties should be subjected to some form of due diligence. This expectation has been communicated to organizations not only through regulatory enforcement actions, but also by way of direct regulatory guidance. In 2012, the U.S. Department of Justice (DOJ) and the U.S. Securities & Exchange Commission (SEC) jointly issued a "Resource Guide to the U.S. Foreign Corrupt Practices Act" (FCPA Guide)[3], which among other things, highlighted the importance of conducting due diligence on third parties. As part of the Guide's *Hallmarks of Effective Compliance Programs*, the regulators specifically noted that "[r]isk-based due diligence is particularly important with third parties and will also be considered by DOJ and SEC in assessing the effectiveness of a company's compliance program."[4]

Regulatory guidance additionally has made clear the expectation that organizations engage in some form of ongoing vetting of their third parties beyond initial screening. The U.K. Bribery Act notes the importance of "continued and regular monitoring,"[5] and the FCPA Guide states that "companies should undertake some form of ongoing monitoring of third party relationships; where appropriate, this may include updating due diligence periodically."[6]

While it is clear that regulators expect organizations to monitor third party relationships for any changes in the corruption risk they pose, they do not offer comparable guidance in terms of what constitutes an appropriate frequency of monitoring.

> **Regulatory guidance has made clear the expectation that organizations engage in some form of ongoing vetting of their third parties beyond initial screening.**

[3] "FCPA Resource Guide," U.S. Department of Justice, https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

[4] "FCPA Resource Guide," p.60.

[5] "The Bribery Act 2010", UK Ministry of Justice, https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

[6] "FCPA Resource Guide," p.60.

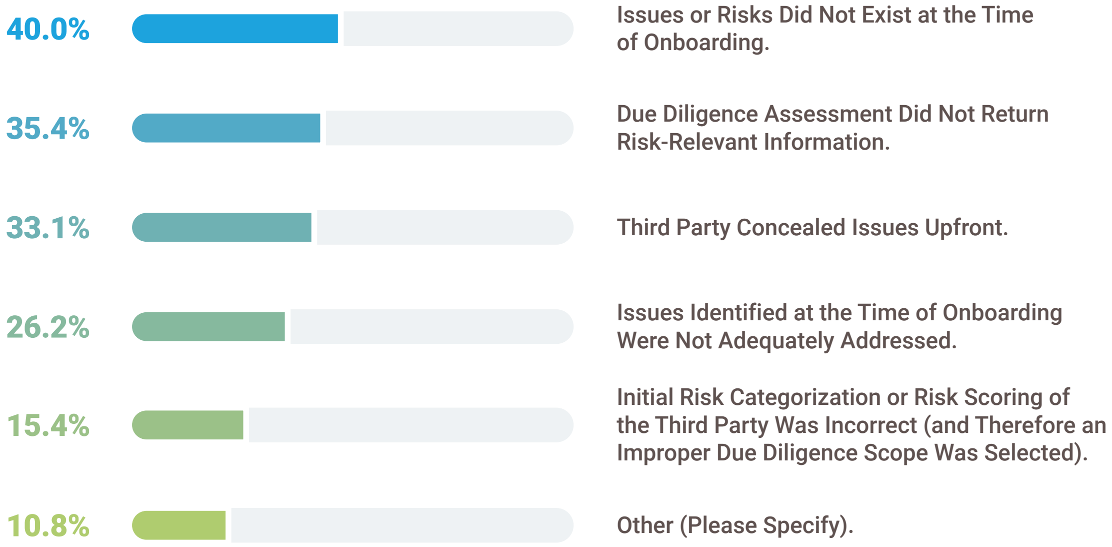
SECTION TWO

CORPORATE EXPERIENCE:
The need to monitor post-onboarding

Companies and their compliance professionals generally have embraced the regulatory expectations when it comes to the idea that some level of vetting needs to be conducted on their third parties. However, in practice, such vetting most frequently occurs only prior to onboarding a third party, not afterward. Not only does such an approach ignore the ongoing monitoring expectations of regulators, it also is at odds with the post-onboarding risk realities that companies face.

As the number and complexity of third party relationships grow, organizations frequently encounter serious issues post-onboarding. In fact, more than half of the survey respondents in the ABC Report indicated they had identified legal, ethical, or compliance issues with third parties after pre-onboarding due diligence had been conducted.[7] When these same respondents were asked to provide a reason why they thought these risks were not flagged earlier, the most commonly cited explanation was that these issues had not existed at the time of onboarding.[8]

Q: If You Experienced Issues With Third Parties Post Onboarding, Why Do You Think This Issue Occurred?



ABC Report survey respondents clearly indicated that pre-onboarding due diligence alone is not enough to adequately address the ongoing risks posed by third parties. Furthermore, companies generally seem to recognize that the solution to the post-onboarding risks rests with some form of ongoing monitoring. Indeed, the most commonly reported means by which organizations discovered that legal, compliance, or ethical issues had occurred after onboarding was actually through ongoing monitoring activity.[9]

Despite the existence of regulatory guidance, and their own business experiences regarding the need to monitor third parties post-onboarding, organizations still must answer an important question: *What should such ongoing monitoring look like?*

[7] Kroll-Ethisphere ABC Report, p. 25.

[8] Ibid.

[9] Ibid.

SECTION THREE

WHAT SHOULD BE DONE?

Regulatory guidance indicates that the role of ongoing monitoring is to "update" – not replace – initial anti-corruption due diligence efforts.

One Size Does Not Fit All

Once a company makes the decision to undertake some form of third party monitoring, it needs to determine what level of ongoing review is appropriate for those particular relationships within the framework of the organization's risk management and compliance standards, policies, and procedures. Each organization has its own mix of third party relationship types, third party population size, and available compliance resources. In order to be effective, it is crucial that any ongoing monitoring plan take into account these and other variables, which will allow a company to absorb information and react in a timely manner to any changes in a third party's risk profile that may come to light as a result of monitoring efforts.

A company's third party relationships can range from the vendor who fills the office soda machines to an in-country agent who directly represents the company in business dealings with foreign government officials. Obviously, the corruption risks posed to an organization by such third parties are very different, and the regulators recognize this. Instead of requiring a company to apply the same level of review to all of its third parties, regulators expect the organization to take a "risk-based" approach to its due diligence.[10] The greater the potential corruption risk posed by a third party, the more comprehensive, and possibly frequent, the corresponding due diligence should be. This risk-based approach to third party reviews should be applied whether in the context of pre-onboarding vetting or post-onboarding monitoring. The key is that it is consistently applied and adapts to any changes in the third party relationship.

[10] "FCPA Resource Guide," p.60.

Due Diligence Versus Ongoing Monitoring

Once a company has established a risk-based approach to monitoring its third parties, the next question is how comprehensive should post-onboarding reviews be? In theory, monitoring solutions could range from basic screenings against relevant sanctions and enforcement lists, to reviews of media sources and public records, to in-country investigative efforts, including source interviews. In practice, however, the more comprehensive levels of review are not practical for most monitoring purposes.

The regulators themselves have drawn a distinction between initial due diligence and that contemplated by ongoing monitoring. Regulatory guidance indicates that the role of ongoing monitoring is to "update" – not replace – initial anti-corruption due diligence efforts.[11] Unlike pre-onboarding due diligence which may occur only once, monitoring by its very nature will extend repeatedly to most, if not all, of a company's existing third party population. Therefore, any monitoring program must take into account the potential scope and frequency involved to fulfill the risk-based approach designated by the organization.

One of the most effective means by which to quickly and repeatedly develop such anti-corruption focused information is to cross-reference a respective third party against publicly available database records. The most common database records searched typically include sanction, embargo, and enforcement watch lists, and politically exposed persons (PEP) lists. This widely used basic screening approach allows for a regular and consistent anti-corruption focused review, although more comprehensive due diligence may be warranted as red flags are discovered. Organizations are well-advised to establish standards for red flag screening to help identify risk thresholds that dictate the scope of due diligence and to trigger the need for more in-depth reviews or investigations.

Continuous or Interval Monitoring

Once the level of ongoing monitoring is determined by an organization, the question becomes at what frequency should the reviews be conducted? Consistent with other regulatory guidance, the FCPA Guide provides only that companies should institute some form of "ongoing monitoring" with respect to their third party relationships. However, the guidance does not specify the appropriate interval at which to conduct that post-onboarding monitoring.

Many companies that look to undertake some level of post-onboarding review immediately gravitate toward the concept of "continuous" monitoring. After all, isn't it better to be constantly updated with possible changes in the risk status of an organization's third parties? Not necessarily.

This risk-based approach to third party reviews should be applied whether in the context of pre-onboarding vetting or post-onboarding monitoring.

[11] Ibid.

It is also important for a company to understand and consider its capacity to process intelligence derived from monitoring activity. A company has an obligation to act in a timely manner on any potentially adverse information which might be developed. If, for example, a third party which previously had no known political exposure suddenly shows up as having a connection to a government official, the company is now "on notice" of this fact and may need to follow up with mitigating action. The time and resources a company can commit to such follow-up, however, is realistically limited. Therefore, an organization needs to consider setting an interval for its monitoring activity which appropriately balances its finite resources with the need to follow up on any red flag. While it is important to be able to demonstrate monitoring efforts to regulators, should an issue arise, it is equally important to show that the company was taking timely action against any flags.

Another factor to consider when contemplating the idea of continuous monitoring is the potential for companies to receive notice of changes in a third party's risk status multiple times per day. In each instance, it can be expected that the company will commit financial and human resources to review, follow up, and document its response in a time-sensitive manner. Exacerbating this realty is the fact that due to the often limited nature of the accompanying identifying information and commonality of many names, screening database "hits" frequently will turn out to be false positives. However, the company obviously will not know which are the false positives at the outset, so it will still be obligated to review and resolve these hits in a timely fashion. This underscores the importance for an organization to develop a highly structured, precise, and automated approach to documenting ongoing monitoring inclusive of risk-based standards which clearly define red flags and any further review and analysis based on this reporting.

Not only can continuous monitoring be onerous in terms of resources expended by the organization, it also does not appear to be required by regulators. As noted above, the FCPA Guide only suggests "some form of ongoing monitoring" be conducted, and where appropriate, only "periodically."[12] Put another way, the regulatory expectation with respect to the required interval of ongoing monitoring is probably more accurately described by the term "interval monitoring."

The appropriate frequency for ongoing "interval monitoring" necessarily will vary from company to company. Much like pre-onboarding due diligence, the considerations will include such factors as the type of relationship, the number of third parties, and the budgetary realities. The appropriate interval, while not mandated, certainly appears to be more than once a year, with common monitoring frequencies implemented at a quarterly, monthly, or weekly rate. Organizations should combine regulatory direction, corporate risk threshold, and available resources to define the appropriate frequency and level of interval monitoring to ensure a risk-based approach that is aligned to stakeholder goals and objectives, and most importantly, appropriately protects the organization from third party risk.

The appropriate frequency for ongoing interval monitoring necessarily will vary from company to company.

[12] Ibid.

Screening solutions enable companies to consistently implement a basic level of ongoing monitoring of their third party populations regardless of size, and to do so at an interval of their choosing.

Scaling Monitoring Efforts

SCREENING SOLUTIONS

As noted above, the goal of monitoring is to update, not refresh, third party risk reviews, and one of the most effective means by which to quickly and repeatedly develop such anti-corruption focused information is to cross-reference a respective third party against publicly available database records.

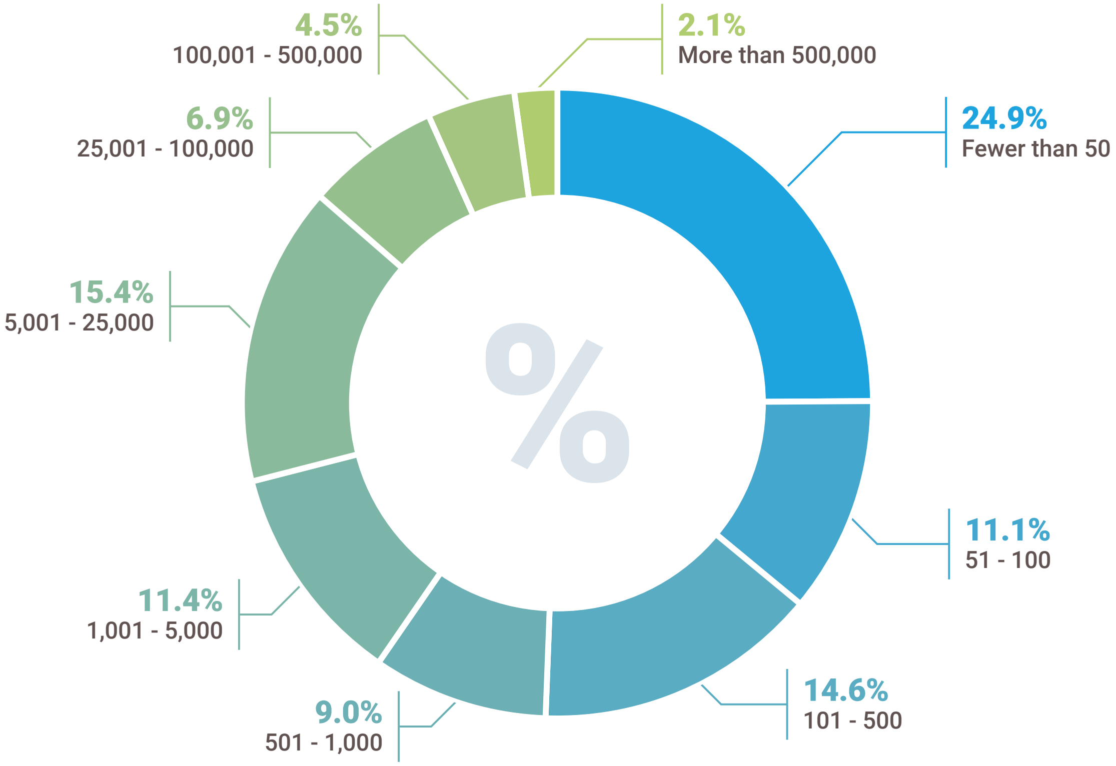
As there are literally hundreds, if not thousands, of geographically diverse corruption-focused databases – both publicly and commercially available – it is not practical for companies to maintain the most relevant and current versions, let alone conduct and review individual searches. Fortunately, there are now many vendors that offer low-cost, high-volume, real-time screening tools which do the work for a company. Aside from the obvious efficiency benefits that such screening technologies deliver, these tools also generally offer a consistent level of review which often extends beyond the basic watch lists and PEP checks. For example, many of the tools include limited searches against various media sources for adverse media mentions.

Screening solutions enable companies to consistently implement a basic level of ongoing monitoring of their third party populations regardless of size, and to do so at an interval of their choosing. Moreover, depending on the screening tool selected, searches can be conducted by the company itself, or outsourced to the screening tool vendor.

TECHNOLOGY ASSISTS

As companies expand their business operations, they have to manage increasingly large and complex third party eco-systems. According to Kroll's ABC Report, more than 40% of the survey respondents indicated they do business with at least 1,000 third parties, and nearly one-third of the respondents confirmed their third party relationships exceed 5,000. Additionally, although in a much smaller percentage, there are companies with third party populations that are greater than 100,000.[13]

Q: How Many Third Parties Do You Do Business With in a Given Year? For the Purposes of this Questionnaire, "Third Parties" Refers to Any Person or Entity You Partner With in Order to Do Business. Please Do Not Include Customers.



[13] Kroll-Ethisphere ABC Report, p. 24.

The obvious challenge faced by organizations that manage these large complex third party networks – or even managing smaller populations with limited resources – is how to do so in a sustainable, cost-effective, and risk-appropriate way. After an organization has a thorough understanding of its desired approach to third party due diligence, it can apply technology to effectively automate and cost-efficiently scale a comprehensive risk-based approach for ongoing third party screening and monitoring.

Not only do technology tools offer a means by which companies can efficiently screen large populations of third parties, they also can be used by companies to incorporate monitoring into their broader third party management process. The more complex an organization's third party network, the more challenging it can be to collect and act upon information about its third parties. This is, in part, because their third parties often operate in multiple jurisdictions and frequently conduct business in local languages.

By leveraging workflow tools, companies can efficiently manage and automate numerous aspects of their third party programs, without geographical or lingual limitations. Some of the most robust third party technology platforms are in the form of vendor-hosted web-based portals, which can be implemented to match the specific third party risk exposure faced by a company. Depending on the type of workflow tool selected, a company can automate:

- the dissemination and collection of initial third party questionnaires;
- its review and risk-ranking of those same third parties;
- the initial due diligence; and
- the escalation of such due diligence efforts when warranted.

Importantly, these workflow tools also can be configured to incorporate the automatic monitoring of the on-boarded third parties at an interval and review level set by the company – and even can include automated annual certification requests and reminders.

By taking advantage of these workflow tools, companies not only have a more efficient way to manage and monitor complex third party populations, but also put themselves in a much more defensible position should they be subjected to any regulatory scrutiny. These technology solutions provide organizations with a consistent and fully auditable approach to managing third party corruption risks, which can clearly be demonstrated to regulators, if needed.

> **By taking advantage of these workflow tools, companies not only have a more efficient way to manage and monitor complex third party populations, but also put themselves in a much more defensible position should they be subjected to any regulatory scrutiny.**

CONCLUSION

Regulators have been unequivocal in their expectation that companies know who they are doing business with. While pre-onboarding due diligence on third parties has become the cornerstone of most compliance programs, many companies are still feeling their way toward integrating effective post-onboarding monitoring strategies. A monitoring approach that is risk-based, scalable, and sustainable can provide companies with not only the ability to uncover potential fraud and corruption within their operations, but also a defensible position should they become the focus of regulatory scrutiny.

Solutions like the Kroll Compliance Portal, which blends powerful technology with human expertise and insight, can help your company maintain an effective ongoing monitoring program on third parties that is customized for your risk thresholds and screening frequencies.

ABOUT THE EXPERT

Robert Huff,
Managing Director,
North America

With a background that includes service with the Federal Bureau of Investigations as well as in private law practice and the corporate sector, Bob has more than 25 years of business development and practitioner expertise within compliance and investigations. Based in Los Angeles, Bob has managed hundreds of civil and criminal investigations, including due diligence matters, both domestically and internationally.

robert.huff@kroll.com | +1 949.383.0809

ABOUT KROLL

Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations, and security through a wide range of investigations, cyber security, due diligence, and compliance, physical, and operational security and data and information management services. Headquartered in New York with more than 35 offices in 20 countries, Kroll has a multidisciplinary team of nearly 1,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals.

CONTACT US

Kroll knows the risk landscape well. Our global team of experts have decades of real-world experience aiding clients with matters related to bribery and corruption, and our offices around the world are staffed with local nationals who are knowledgeable in their countries' business, political, social, and economic landscapes. The combination of these capabilities and resources, along with our flexible technology platform, helps maximize your company's ability to identify current vulnerabilities and anticipate areas of risk to support more successful ventures.

Please contact us to connect with one of our local experts to discuss your compliance and due diligence needs, whether you are looking for support in enhancing compliance and due diligence programs or establishing new strategies, like an automated monitoring program.

information@kroll.com
kroll.com/en-us/what-we-do/compliance

Kroll®

kroll.com/en-us/what-we-do/compliance

Statements herein concerning financial, regulatory or legal matters should be understood to be general observations based solely on Kroll's experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which Kroll is not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas.