Diligent

Ongoing Monitoring

Managing Third-Party Risk Amid Global Uncertainty

To learn more about Diligent Compliance solutions or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com

INTRODUCTION

In an era of vast complexities and uncertainties, third-party risk remains one of the most significant compliance threats to modern companies. This environment of volatility has reinforced the need for businesses to enhance their third-party oversight techniques and to monitor market changes more diligently. Recent updates to the DOJ guidance have also emphasized a greater expectation for companies to engage diligence beyond the initial onboarding.

In June of 2020, the DOJ published a revision to its Evaluation of Corporate Compliance Programs. Within its new guidance, the issue of ongoing monitoring was addressed specifically with regards to third-party management, asking if the "company engage[s] in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?" The way the DOJ worded this question suggested the answer. Certainly, for high and perhaps medium-risk third parties, periodic review of the third-party relationship would be the reasonable course of action, perhaps coupled with continuous monitoring of the third party against global sanctions, watchlists and negative news databases.

But the answer to this challenge demands even more than simply adopting the latest third-party gadgetry. While technology has without question revolutionized how compliance professionals conduct third-party oversight, the world's leading programs know that any computerized solution is only as good as the people who operate it. When building an effective third-party management system, the most effective compliance programs always leverage both human and artificial intelligence, combining advanced technologies with expert analyses to provide valuable risk insights. This integrated approach is precisely what global enforcement authorities have come to expect amid these new frontiers of global change.

Fortunately, today's compliance leaders are developing advanced due diligence and monitoring techniques that combine the very best of third-party data and time-tested compliance know-how. Proactively building systems to identify and protect against third parties' bad behaviors will place your company well on the path toward more useful risk insights. The organizations unafraid to update and enhance their due diligence, monitoring and investigative capabilities will be empowered to safeguard their cultures, reputations and bottom lines. This white paper explores these trends and provides a roadmap for proactive third- party programs seeking to modernize their third-party monitoring. From the war in Ukraine to post-COVID hybrid work environments, only those who appropriately respond to today's fluid risk environment can traverse the unknown — whatever it may hold.

DYNAMIC RISK ENVIRONMENTS REQUIRE ROBUST THIRD-PARTY MONITORING

The global health crisis of the past few years has given way to geopolitical and economic uncertainty, creating major disruptions previously unseen in our modern era. With change as the only true constant into 2023 and beyond, compliance professionals must find ways to prepare their third-party monitoring to tackle a host of emerging challenges:

- **Political and market disruptions**: Geopolitical instabilities and market volatility brought on by Russia's invasion of Ukraine are interfering with global business practices and supply chains. Resulting trade sanctions have also forced businesses to be proactive in managing compliance.

- **Rising social consciousness:** Customers, stakeholders and employees alike are increasingly demanding social justice. Companies must reinforce their commitments to shared principles like ethical cultures and honest business practices. Doing the right thing, of course, is good for the world and good for business. Principled organizations are always better equipped to contend with unforeseen third-party risks.

- **Rise in misinformation and unreliable sources**: Events like the January 6 riots have reminded us of what can happen when political propaganda and misinformation are multiplied among the masses. As social media takes root as a primary mode of communication, this mass interconnectedness has multiplied the numbers and types of sources from which people derive information — much of it unreliable. The decentralization of knowledge through the internet has allowed bad actors to infiltrate the airwaves with anonymity, and offered little recourse for the spreading of mistruths and outright lies. These developments clearly underscore the importance of relying on trusted partners with experience and expertise in their field.

- **Heightened regulatory expectations and unpredictable enforcement patterns**: Top global enforcement agencies have signaled that not even the most ingrained institutions will be safe from legal enforcement, as the U.S. government's antitrust case against Google is set to go to trial in late 2023, while the FTC pursues similar actions against Microsoft. Every company is potentially vulnerable. Your business needs to know when a third party, or its owners or managers, end up arrested, indicted or placed on a watchlist.

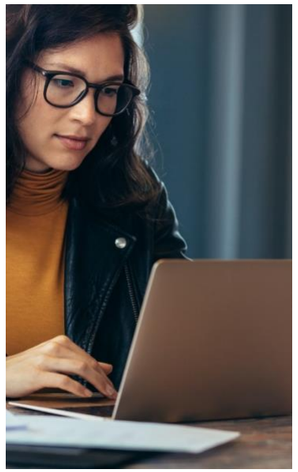
- **Foreign policy changes**: Shifting foreign policy decisions continue to alter the course of global geopolitical relations, causing routine, often erratic, disruptions to lists of sanctioned parties and high-risk enterprises.

As sanctions against Russia, China, Iran and others continue to pile up, complex owner structures and multiple layers of shell companies create waves of new compliance hurdles for many companies with extensive international operations. These rapid swings in the applicable rules are becoming more common, and their stark ripple effects bear directly on your company's success.

- **Evolving role of compliance itself**: In light of these evolving risks, many organizations are expanding the role of compliance itself to add functionality and value. These changes are compelling compliance officers to wear more hats than ever. In the years to come, the compliance function will become even more embedded within companies' core operations. As such, top compliance programs will continue to need sharp, dedicated and experienced teams to see them through these challenging and uncertain times.

As these evolutions make it increasingly difficult for company leaders to observe their third parties' behaviors in real time or in sufficient detail, they are reordering many companies' traditional third-party risk analyses and risk-management priorities. As such, the lurking uncertainty ultimately highlights the need to monitor and scrutinize third parties more closely, and reinforces the need for strong third-party due diligence measures. Accelerated rates of change necessitate tighter procedures and renewed due diligence at more frequent intervals, because changes are happening all the time. Those who do not maintain constant visibility in real-time will inherently miss critical updates. Navigating novel global forces thus requires renewed third-party monitoring strategies focused on resolving risks proactively before more concerning problems can materialize.

It is easy to see how new issues can arise. Today's world consists of a constant, unending stream of new data generated through seemingly limitless platforms, sites, forums and networks across cyberspace every day. When so much changes in so short a period, the process of prioritizing third-party risks, screening third parties through major global databases, investigating red flags and designing sufficient third-party controls is only the beginning. When every single news story generated, court case filed, watchlist updated, deal struck or image posted — every drip of new content — could impact your company's risks, reputation and bottom line, the sheer scale of new information produced even within a passing moment can feel staggering. Seasoned compliance practitioners know that their responsibility to manage



third-party risk does not end after a third party is onboarded. New sources of risk can and do arise, often from third parties whom you have known and done business with for years.

In this fluid and dynamic risk environment, swift and precise action is critical to sustained business success. Compliance teams are thus compelled to embark on a continuous journey to uncover and piece together new information about their companies' business partners at a moment's notice. The pressure is certainly on. Clearly, companies will continue developing and depending on their third-party practices to ensure the entire organization can operate free of sinister parties and costly legal pitfalls.

ARTIFICIAL INTELLIGENCE SHOULD COMPLIMENT HUMAN INTELLIGENCE

Today's leading compliance programs must integrate both human and machine elements, and enhancing their third-party procedures still demands more than sophisticated compliance technologies alone. The world's leading compliance programs understand the balanced relationship needed between technology and the people who operate it. No matter how sophisticated the applicable technologies may become, it is human beings who drive true change toward the future. Put simply, automated platforms must be backed by human skill, capability and dedication.

The question of artificial intelligence versus human intelligence, however, is not a competition; it is a balancing act. AI-based systems should be designed to complement the capabilities of expert analyses. Certain types of third-party red flags are almost impossible to spot with the naked eye — for instance, the presence of restrictive economic sanctions or negative media articles that are embedded within massive quantities of data constantly churning through cyberspace. In these instances, computerized intelligence and machine learning excel at scanning the regulatory horizon to spot concerning trends — effectively turning a Herculean task

into a standard process. But those datapoints must then be evaluated, questioned, explored and documented before a thorough and informed risk decision can occur. So, a knowledgeable and experienced team of experts is still necessary to piece together broader datapoints to connect the dots and yield useful insights.

It is also worth remembering that international criminals do not typically advertise their corrupt acts for government watchlists to catalogue publicly in detail. As such, concealed, non-public information is often critical to truly understanding your third parties' qualifications, capabilities and associations. Obtaining beneficial ownership information, investment sources, banking relationship information, key business associates, names and locations of customers and suppliers, and litigation records all requires human-led interventions and in-depth investigative procedures. Moreover, during higher-risk scenarios, no computer program can physically supplant boots-on-the-ground site visits. Going beyond publicly-accessible information, when necessary, enables investigators to develop context, connect the dots, and ensure that company leaders make accurate, valid, reliable and informed risk decisions.

Regardless of how advanced our technologies may become, only human intuition can uncover and decide, for instance, a vendor's true capacity to complete the work it was contracted to perform, or a business partner's true reputation for ethical business practices. Once the machines have generated our most reliable data, it is the humans who must synthesize the available datapoints to calculate the likelihood of lurking risk. The complex problems and unexpected events of our modern world will always require strategic brainstorms, collaborative plans, and coordinated execution by teams with localized knowledge and skilled insights. Compliance technologies exist to augment, not replace, these fundamentally human endeavors.

Additionally, so much of compliance is focused around building principles of ethics and integrity into the organizations we represent. With the nature of threats evolving worldwide, it is people, not the machines we operate, who are ultimately accountable for failing to root out wrongdoing within our companies. Particularly through an age of rampant misinformation, only we as compliance leaders have the capacity to build transparency, accountability and procedural safeguards into our organizations' structures and processes. Third-party due diligence should be about people throughout the company working across silos to escalate truthful

information, and helping one another to safeguard the common enterprise from whatever the outside world may hold. To do this requires dedicated teams focused around trust. Before any machine can crunch an algorithm, we always must begin with that shared human commitment to progress and truth.

In today's risk environment, humans of integrity will pave the future. Technology's algorithmic calculations, by their very nature, carry limitations in their sensitivity and intuition, and they may be susceptible to bugs, typographical errors or other data lapses. Compliance personnel who over-rely on technology or "set it and forget it" will leave their companies exposed to oversights that may spell disaster down the road.

With challenging times surely ahead, the new frontier of third-party compliance will entail deeper, more refined monitoring techniques to identify potential misconduct earlier and to remediate compliance deficiencies more completely. Your third parties' legal, financial and reputational risks are your risks too, so do not be lulled into a false sense of security. The ultimate accountability for implementing effective third-party techniques falls squarely on the organization's board of directors and executive management. Compliant third-party monitoring processes entail more than entering a name into a screening search bar, checking it off a to-do list, and walking away; it requires an innovative action plan to appropriately monitor third-party risk. The following key strategies can help compliance teams ensure their monitoring programs are fully prepared for what lies ahead:

- **Certifications and questionnaires**: Third-party questionnaires and certifications are extremely useful tools, and investigative teams can submit them for completion to any third party at any time throughout the business relationship to verify needed information. Nothing prevents a company from asking a third party to update a questionnaire during its contractual term, and compliance personnel should utilize these opportunities for enhanced visibility. Many companies mitigate risk by requiring more frequent compliance certifications for their higher-risk agents and distributors. Any attempts by the third party to resist these routine certifications or requests for information may amount to additional red flags and datapoints.

- **Contract renewals and reviews**: Whenever a third party's contract has expired and is up for renewal, do not miss the opportunity to refresh its due diligence screening. In many cases, seeing no glaring issues with the third party, organizations will ignore this opportunity and quickly sign a renewal contract on the same terms and conditions as the initial agreement. This is a mistake, as much can change in short order. Ensure that your organization takes a step back to reexamine its business relationships at these critical junctures by collecting valuable experiential data about the third party's performance, compliance efforts and overall business utility thus far. Study the third party's current legal status closely to ensure nothing significant has changed since the initial onboarding due diligence was conducted, and document the results within a centralized location.

- **Financial controls**: Between renewal intervals, companies should monitor third parties' compliance with the specific contractual requirements to which they have agreed. This may occur through internal verifications that the responsible parties within your company are receiving the services contracted and that the third party is adhering to the applicable invoicing procedures. Your accounts payable personnel should play a critical role here by reviewing invoices and elevating potential issues, including inflated bills, suspicious funds or rebates, and sham contracts. Any sales or operations personnel who interact with the third party should also remain alert to note any red flags or issues that may surface and require follow-up inquiries.

- **Audits**: Companies should have a variety of auditing techniques at their disposal to conduct periodic and ongoing third-party reviews. Since the nature of broader, formalized audits can limit their frequency and usefulness, modern approaches should include a mixture of informal spot checks, transaction sampling and monitoring, and broader formalized audits, with a focus on high-risk transactions, jurisdictions and business functions. Companies can no longer rely on occasional third-party audits to satisfy monitoring requirements. Compliance professionals must work closely with auditing partners to develop appropriate strategies that attain these goals. It is advisable, for instance, to secure audit rights in written contracts with third parties and to exercise those rights on a periodic basis. If a third party resists or refuses an audit, you should reexamine the business relationship immediately.

- **Test and update**: Organizations are responsible for regularly testing, evaluating and updating their procedures to address any weaknesses that may arise. Incorporating some manual review of this nature provides your automated systems with a human backstop. To conduct this review, your organization should document why it selected a particular automated system, how it calibrated that system to conform to its specific risk profile, and whether it has tested the technology's accuracy. This testing should occur both at the enterprise-wide level and within specific divisions, and it should be aimed at remedying any gaps identified through your broader monitoring strategies. Work closely with software specialists to optimize your technology's performance, keep the programs up-to-date, reduce the potential for software errors to occur, and ensure that your organization understands how the program is performing. If and when issues do occur, customize and tailor control measures to account for changing risks and to fix the root cause of the compliance defect.

- **Respond nimbly**: Today's legal frameworks place great emphasis on the need for compliance programs to adjust rapidly. Sanctions and corruption watchlists are revised on short notice, and new public guidance documents may be issued at any time. Whenever possible, establish routine workflows that incorporate automated notifications and on-demand updates of any risk changes. If and when these changes do occur, your company must work to restore balance swiftly. Work toward contingency plans with clear executive summaries that interpret the key action items, prioritize the activities requiring greater resources, explain how to respond, remedy impacted business areas and identify who is responsible for each component of the response. This makes communication and interaction throughout your monitoring system a streamlined exercise that benefits compliance outcomes.

- **Make it routine**: Monitoring and managing third-party risk is an ongoing series of processes, beginning with the initial business engagement but enduring throughout the business lifecycle. Develop roadmaps and compliance calendars for your organization's contracts, policies, procedures, training programs, audits and assessments to ensure all potential risk is accounted for. Put simply, make a schedule, keep up with the times and stay sharp. Do what you can to attain synergies, minimize guesswork, and make the processes more predictable. These measures build further trust among employees and ensure that compliance is viewed as an asset throughout the organization.

- **Make it a team effort, and think big-picture**: The most effective monitoring programs are developed as coordinated efforts among compliance, legal, audit, finance and procurement staff, engaging key stakeholders to build a community of subject- matter experts and compliance advocates across the business. Top programs know that compliance results demand a holistic approach with involvement, awareness and buy-in throughout the organization. Remember that third-party compliance is a common goal that benefits everyone throughout the organization. In this common pursuit, culture counts. Consider branding compliance to include a clear focus on ethical principles. Organizations with strong cultural commitments to doing right always fare better overall.

- **Follow the risk**: The amount of work needed to comprehensively monitor your organization's risks may sound daunting, but risk-ranking approaches and sampling techniques should guide the way when tailoring your company's monitoring function to its available resources. As we have seen, third-party relationships do not exist in a vacuum. Organizations must constantly reassess the nature and extent of their third-party risks to prioritize the greatest risk areas. Familiarize yourself with the common red flags and high-risk scenarios that third parties may present.

POWERFUL DATA PROCESSING TAKES THIRD-PARTY COMPLIANCE TO THE NEXT LEVEL

These developments have been loudly echoed by government enforcement authorities worldwide, who continue to demand stricter penalties from organizations that fall short. Prevailing regulatory standards have also suggested companies leverage data in adopting strategies for faster, more accurate and more consistent third-party monitoring strategies. Moving forward, as harnessing data transitions from an advantage to a requirement, companies must devise more innovative and inclusive ways to incorporate data analytics into their third-party programs. To illustrate this point, the United States' latest guidance on evaluating compliance programs lists a number of open questions that prosecutors must consider when investigating organizations and determining whether to file criminal or civil charges:

- What collection and analysis of compliance data does the company undertake?
- What types of information or metrics has the company collected and used to help detect the type of misconduct in question?
- How has information or metrics informed the company's compliance program?
- How does the company monitor its third parties?

- Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and testing of policies, controls and transactions?
- Do any impediments exist that limit access to relevant sources of data?
- What is the company doing to address impediments to relevant sources of data?
- Does the company track red flags that are identified from third-party due diligence and how those red flags are addressed?
- Does the company track which third parties do not pass the company's due diligence, and does the company take steps to ensure they are never rehired later?
- How has the company collected, tracked, analyzed and used information from its reporting mechanisms?
- Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?
- Have periodic reviews led to updates in policies, procedures and controls?
- Are periodic reviews limited to a snapshot in time, or are they based on continuous access to operational data and information across functions?
- What testing of controls does the company undertake?
- Does the company review and adapt its compliance program based upon lessons learned from the misconduct of other companies facing similar risks?
- Does the company have a process for tracking lessons learned?
- How are results reported and action items tracked?

CONCLUSION

Recent years have seen the culmination and convergence of a number of long-developing global trends, each carrying direct implications for compliance practitioners worldwide. The speed of change is requiring organizations to adapt to transformations that are producing new market necessities, updated legal requirements and shifting consumer preferences. As volatile global trends have produced uneven patterns of third-party risk and legal enforcement, numerous companies have suffered penalties due to their failure to adequately monitor third-party activities.

Global restructuring and reordering, of course, in no way relieves organizations of their responsibility to comply with the law. To the contrary, proactive and swift action is now even more critical, and tight monitoring procedures have become key to sustained compliance success amid a chaotic world. As organizations look ahead to 2021 and beyond, the expectations and the stakes are markedly higher. Savvy compliance professionals must define for their organizations where they stand and where they will go from here. Those who are bold enough to rethink their third-party monitoring protocols will develop the right strategies to better understand their risks and keep their organizations safe.

Increasingly, companies understand that third-party risk cannot be managed without the appropriate balance of technology and human expertise. The power of integrated third-party platforms must complement the depth of sharp investigative skills and resources. Faster and more dependable validations of third-party credentials must accompany deeper investigative inquiries into concerning red flags and data patterns. The key is finding the right partners who seamlessly blend both human and artificial intelligence to harness maximum safety and security during these turbulent times. By simultaneously embracing new technologies and constructing broader coalitions to better monitor risk, organizations can gain timely and consistent access to reliable information, all while maintaining the deep insights from trusted experts. This leaves those organizations prepared to contend with a broad range of risk scenarios, and it separates top-tier third-party monitoring programs from all the rest. Tackling third-party risk in today's complex risk environment requires a wide-angle view and a forward-thinking mindset. Overall, those who take care to implement the recommendations outlined in this white paper can take solace in knowing that their companies can and will address the challenges of today and beyond.

Building a credible and defensible compliance program is vital for ensuring compliance with global regulatory statutes. It requires a multi-pronged approach that aligns to your organization's people, processes and technology in order to not only prevent and detect violations, but to foster a culture of integrity within your company. Diligent offers configurable compliance solutions that help businesses to thoroughly evaluate and mitigate potential risk. To learn more about Diligent's Ethics and Compliance platform, click here.

ABOUT DILIGENT CORPORATION

Diligent is the leading governance, risk and compliance (GRC) SaaS provider, serving more than one million users from over 25,000 organizations around the globe. Our modern GRC platform ensures boards, executives and other leaders have a holistic, integrated view of audit, risk, information security, ethics and compliance across the organization. Diligent brings technology, insights and confidence to leaders so they can build more effective, equitable and successful organizations.

Diligent
info@diligent.com
www.diligent.com