COMPLIANCE WEEK

2019

Survey on Anti-Bribery & Corruption

SPONSORED BY

REFINITIV™

DATA IS JUST
THE BEGINNING

Table of contents

Executive summary

The 2019 Survey on Anti-Bribery & Corruption was conducted jointly by Compliance Week and Refinitiv over the course of two months in early 2019, generating 233 total responses from anonymous compliance and risk professionals and revealing some surprising (and a few alarming) trends.

The survey was comprised of 20 questions and was broken up into three parts: a basic benchmarking of a respondent's anti-bribery, anti-corruption program; a look at how companies evaluate and monitor third parties (including a deeper dive on enhanced due diligence); and an evaluation of training programs with a particular focus on automation and advanced technologies.

What follows are key takeaways from each section:

Basic benchmarking

» About two-thirds of those surveyed rated the effectiveness of their anti-bribery program either a 4 or 5 (on a scale of 1-5, with 5 being most effective), with just 12 percent giving themselves a 1 or 2.

» Overall, 67 percent of respondents indicated they had adequate resources to ensure the success of their anti-bribery program.

» Nearly 80 percent of respondents expect their bribery and corruption risks will either increase or remain the same over the next 2-3 years.

» What types of misconduct do compliance officers define as corruption? Of the eight options, the most common selections (respondents could choose all that applied) were bribery, fraud, money laundering, price fixing, and bid rigging, all garnering the votes of more than 50 percent of practitioners who took the survey.

» Perhaps the most encouraging result: 87 percent of respondents say their companies have programs in place that encourage whistleblowers and thwart retaliation.

Third parties and "enhanced due diligence"

» The most concerning result was that 38 percent of those polled indicated they never train their third parties on anti-bribery and corruption. Among that group, 28 percent indicated they expected their ABC risk to increase over the next 2-3 years and a whopping 43 percent said they have third parties operating in high-risk or sanctioned jurisdictions internationally. (Overall, just over 50 percent of respondents said they have partners doing business in high-risk areas.)

» Almost everyone whose job it is to ensure quality training for third parties will tell you that nothing can replace boots-on-the-ground, in-person training, even for international entities. Just 30 percent of those polled, however, conduct on-site anti-bribery/anti-corruption training for their third parties. Among companies that indicated they have third parties that operate in high-risk areas internationally, that number creeps up to 33 percent.

» The most likely reason a third party will fail to meet an organization's standards is "general reputational or integrity concerns" (se-

Perhaps the most encouraging result: 87 percent of respondents say their companies have programs in place that encourage whistleblowers and thwart retaliation.

lected by 56 percent of respondents), followed by "unusual contract and payment structures" (36 percent), "suspect corporate structures" (28 percent), and "questionable relationships with politically exposed persons" (27 percent).

» The biggest factor in a company's decision on whether "enhanced due diligence" is needed for a third party is geographical risk, according to the survey, followed by past behavior and industry-related risk.

» Overall, 54 percent of those polled said less than a quarter of their third parties undergo "enhanced due diligence"—by far the most popular answer. About 13 percent indicated that none of their third parties undergo that level of extra scrutiny.

» The added cost of enhanced due diligence is the biggest challenge for companies, according to the poll, followed closely by a "lack of knowledge."

The biggest factor in a company's decision on whether "enhanced due diligence" is needed for a third party is geographical risk, according to the survey, followed by past behavior and industry-related risk.

Effectiveness and automation

» Companies seem to be better at training domestic employees on rules and procedures than they are at doing the same for their international workers. About 62 percent of those polled gave themselves the equivalent of an A or B when asked to evaluate how effective they were at training U.S.-based workers. Internationally, less than 50 percent of respondents gave their companies those same grades.

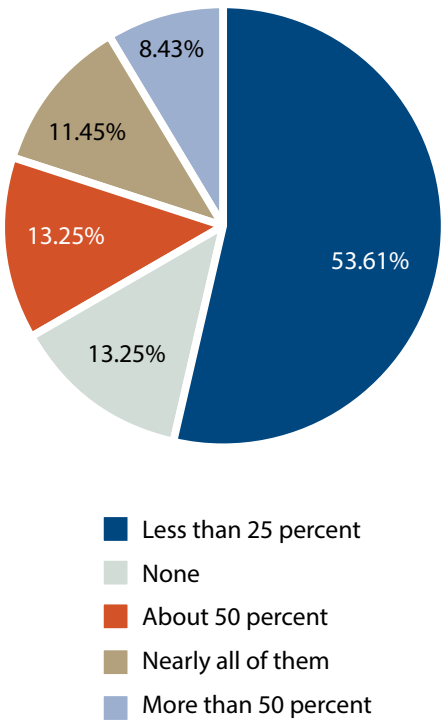
» It seems most companies polled have automated processes in place to carry at least some of the load for their anti-bribery programs. Those polled were offered five answers to a question about which parts of their programs were automated, and each of the five got a check in the box from at least 30 percent of respondents. Training domestic employees (51 percent) and monitoring and certifying third parties (43 percent) were the leading vote-getters.

» While the rate of adoption for automation was high, the same cannot be said for emerging technologies. We asked whether companies were using or planning to use artificial intelligence, blockchain, or machine learning to enhance their anti-bribery programs, and a surprisingly high 67 percent answered "none of the above." AI was next at just 21 percent. ■

SECTION 1

How to determine when enhanced due diligence is warranted

What percentage of your third parties undergo "enhanced" due diligence?



It can cost time and money and could even drown a deal. So when do the challenges and costs associated with this step outweigh the risks of not doing it?

By Joe Mont

In the compliance world—especially as it relates to deal-making and neutralizing corruption—due diligence is risk assessment commandment. When, however, is enhanced due diligence warranted? What motivates firms to decide if a third party should undergo an even stricter, more refined level of scrutiny? What are the costs and challenges?

The importance of enhanced due diligence is borne out in results from the recently completed Compliance Week survey on anti-bribery and corruption, conducted in conjunction with Refinitiv.

The pitch for an EDD program is a straightforward one: No enhanced due diligence investigation is ever the same. By undertaking a detailed review of new and existing customers and third parties, you can help guard against reputation and regulatory risk.

Nearly 90 percent of respondents to the survey said they put at least some of their third parties through these enhanced reviews with an eye toward safeguarding their reputations and complying with both foreign and domestic legal demands. The goal: reducing uncertainty and risk and making more informed, safe, and profitable business decisions.

Among the questions asked in the survey: "What percentage of your third parties undergo enhanced due diligence?"

A mere 13.25 percent said they do no such added screening. That same percentage indicated they put 50 percent of their third parties through enhanced due diligence. About 53 percent of those surveyed performed EDD on less than 1 in 4 vendors and about 20 percent put more than half of their third parties through enhanced vetting.

What were the biggest challenges firms face at the enhanced due diligence stage of their screening process? Responses (from 166 compliance professionals surveyed) included cost of enhanced checks (30.7 percent); lack of knowledge (31.3 percent); delivery time (16.9 percent); and data security (14.5 percent).

On a scale of 1-5 (where five was the strongest), respondents were asked which factors weighed heaviest in their decision on whether enhanced due diligence was needed. Top answers included geographical risk, political risk, industry-related risk, past behavior, and the importance of the third party to the business.

To grasp when enhanced due diligence—increased screening and analysis of otherwise standard data collection—is necessary, we turned to Kevin Bogdanov, director of market development – risk, Americas, for Refinitiv's customer and third-party risk management business. He is currently exploring how data, technology, automation, and AI will disrupt and redefine of Know-Your-Customer and third-party risk compliance.

"Enhanced due diligence really just fulfills a role within a certain stage of the due-diligence cycle," he says. "You've got a risk assessment that your company will usually leverage and using that assessment you will determine what is risky for your business, in terms of cyber-security, inquests, bribery, corruption, or whatever. So, off the back of that, you might want to determine where there might be heightened exposure that requires greater due diligence to make sure that you really go out to those problematic areas."

"These are just a couple of examples," he adds. "But if any of these criteria or a combination of these criteria exist, then that is going to necessitate a greater level of due diligence. You would ideally have a risk matrix and risk assessment from the onset to determine what matters to you in terms of where your risk is and then, if any of those criteria are established in the available data, you would obviously go ahead and warrant some deeper diligence."

Steadfast supervision

Once committed to that process, does enhanced due diligence retain a given life span? The answer: "sort of."

"There is a process here, an end process, ideally," Bogdanov says. "Obviously, you can't sort of screen, or take your diligence at a point in time, and assume that nothing changes. However, if you just look at a couple of examples of things that can change—ownership structures, loans, joint ventures, new product lines, and new markets that the businesses will enter—any one of these changes may be a trigger. Another big one is mergers and acquisitions."

"Any of these types of changes will fundamentally upend in the level of risk and the type of risk that is inherent in a third party. So, what you need to do is you need to establish a cadence and framework for continuous monitoring of those parties."

Most probably won't need to do a refresh that often, because it would likely be classified low risk—unless some other factors elevate it. "Whereas if you have a high-risk entity and high-risk part of the world, maybe you might need to do the refresh as often as every year, for example," he says. "You will, however, probably need to go and again issue a questionnaire and more than likely undertake independent analysis or leverage your data sources. You could look at changes in the media landscape, as there may be some sort of media article outlining potential hazards."

"A firm may also want to create real-time alerting around changes in ownership structure, or new flags in a high-risk database."

There is, nearly all experts warn, a cost to enhanced due diligence. To screen somebody in a database might cost you $1 a record or more. So there is a risk in thinking enhanced due diligence is always going to be better. Sometimes, it's overkill.

"We have definitely seen over-screening and over-due diligence," Bogdanov says. "It works equally on both ends of the spectrum. You need to have established the right framework and the right risk threshold upfront." ■

On a scale of 1-5, how much do each of these factors weigh in your decision on whether "enhanced" due diligence is needed?

Weakest <———————> Strongest	1	2	3	4	5
Geographical risk	13.25%	4.82%	18.07%	21.08%	42.77%
Political risk	19.28%	18.67%	19.88%	16.87%	25.30%
Industry-related risk	12.65%	10.84%	26.51%	25.30%	24.70%
Past behavior	10.84%	7.23%	24.10%	22.89%	34.94%
Importance of the third party to the business	15.66%	12.65%	32.53%	15.66%	23.49%

Poll shows room for improvement on training third parties

Results from the Compliance Week and Refinitiv survey revealed some surprising facts about companies' third-party training; based on those results, the following article offers suggestions for how to enhance the process.

By Jaclyn Jaeger

Chief compliance officers and chief risk officers worth their salt know the myriad compliance risks that third parties pose to their companies, and so it shouldn't come as a newsflash that training third parties is an essential part of a robust compliance program. Even knowing that, however, many companies today still don't train their third parties, leaving themselves vulnerable to bribery and corruption risk.

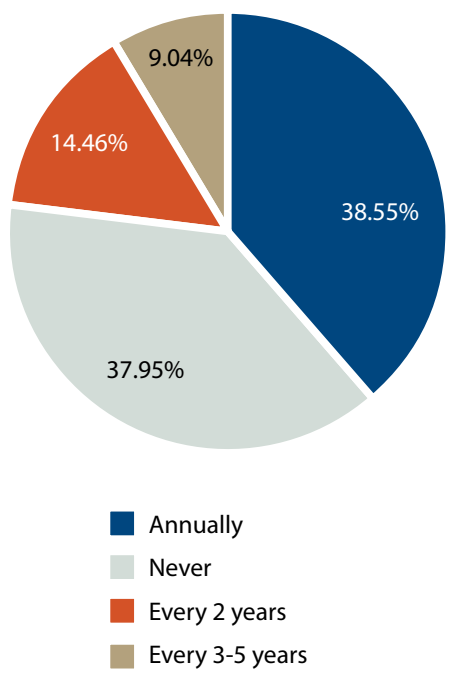
That was just one of many key findings to come from a recent anti-bribery/anti-corruption (ABAC) benchmark report conducted by Compliance Week, in partnership with Refinitiv (formerly the Financial and Risk business of Thomson Reuters). According to the findings, 38 percent of risk and compliance officers polled said they have never trained their third parties. This finding is particularly concerning given that more than half of respondents (52 percent) said they have third parties based in, or operating in, high-risk or sanctioned jurisdictions globally.

Equally pressing is that enforcement agencies in the United States and elsewhere around the world expect companies to train their third parties as part of a robust compliance program. The 2012 FCPA Resource Guide, for example, specifically states that "companies should undertake some form of ongoing monitoring of third-party relationships. Where appropriate, this may include updating due diligence periodically, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party."

On a practical level, compliance departments must overcome a variety of obstacles that may explain, in part, why so many companies still don't train their third parties, including lack of resources, time, and budget; potentially a lack of support from senior management; a desire to "move the needle forward" as it relates to business; and/or not recognizing the potential risk that a third party poses.

On a positive note, 62 percent of survey respondents said they do train their third parties on their anti-bribery and anti-corruption compliance program in some fashion. Among these respondents, the plurality (38 percent) said they train their third parties annually, while 15 percent said every two years, and nine percent said every three to

How frequently do you train your third parties on anti-bribery and corruption?



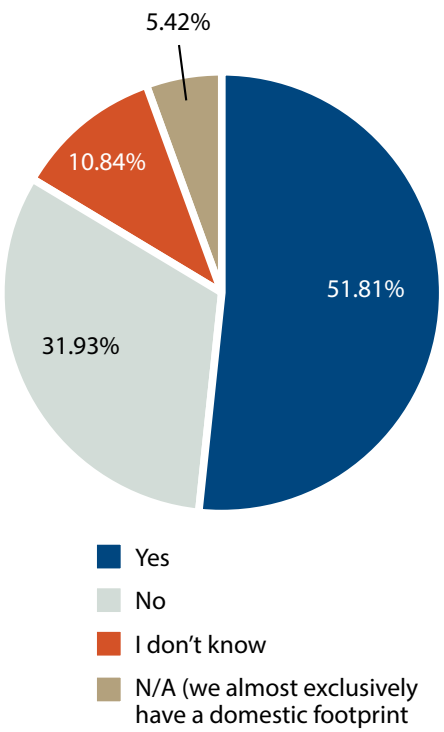
five years.

Survey respondents further indicated that they train and educate their third parties on anti-bribery and corruption issues through a variety of means, including:

» Distributing or posting printed materials for employees to review (39 percent);
» In-person or on-site training (30 percent);
» Online or Web-based training (46 percent);
» Including certification in contract materials (34 percent);
» Making it part of an onboarding questionnaire (40 percent); and
» Including an anti-bribery statement in the Code of Conduct policy (64 percent).

Done right, the delivery methods used to train and educate third parties should be dictated by certain factors. For a domestic distributor that poses a low risk to the business, for example, online training and self-certification upon completion may be enough, whereas a third-party intermediary operating in a high-risk jurisdiction may require in-person training. "Everything should be predicated on the risk assessment," says John Arvanitis, a managing director in the Compliance Risk and Diligence practice at Kroll.

Do you have third parties based in (or operating in) high-risk or sanctioned jurisdictions internationally?



Relying on the risk assessment

What third parties pose the highest risk in the supply chain? Where are they located? "The training should always be appropriate and should be based on the risk assessment that's conducted and potentially the risk profile that the business faces in the jurisdictions or industry in which it operates," Arvanitis adds.

Just as delivery methods of third-party training will vary, so should the subject-matter of that training. This means ensuring that the training is "specific and relevant," Arvanitis says, "rather than providing a litany of information that may not be impactful or substantive for the third party."

Sales distributors, for example, often need training on anti-bribery and anti-collusion risk, whereas technology vendors need training on data privacy and cyber-security risk. Cultural nuances are another factor: Certain gifts and entertainment that pose a common bribery risk in one country may not pose any risk in another country.

Evaluating or monitoring the effectiveness of third-party training is also important. When asked how they follow up on third-party training, respondents gave a variety of answers, including attestations (37 percent); in-person meetings (35 percent); questionnaires (32 percent); and auditing (29 percent).

One way to evaluate the effectiveness of third-party training is to include a scenario-based quiz at the end of the training course. Asking third parties how they would handle a certain situation will garner much deeper insight than merely asking them the definition of a bribe, for example. Another helpful metric may be to track the rate of

inquiries made by third parties to the compliance department in the days and weeks following the training.

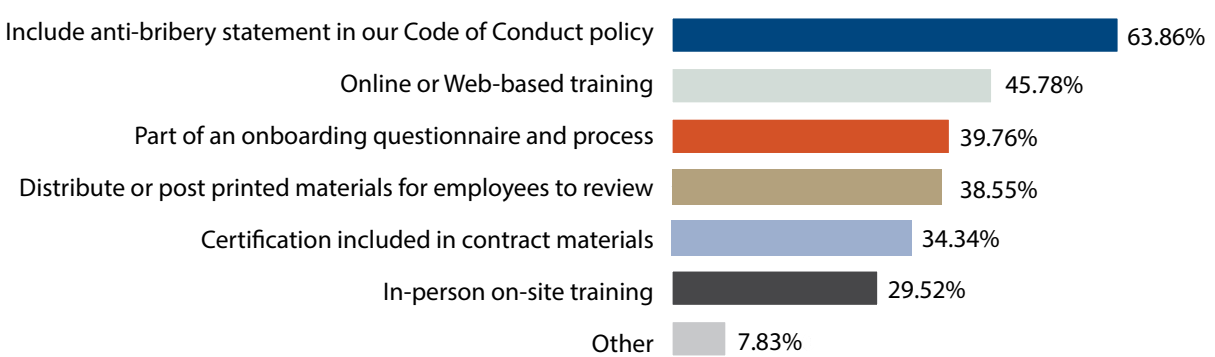
It's also important to periodically reassess third-party risks so that the training stays aligned with changing risk profiles. Third parties that do not pose a high risk today may pose a high-risk tomorrow, as new products and services are added, executives rotate, or allegations of misconduct come to light.

Above all else, however, because compliance teams cannot effectively train third parties without knowing their third parties or the specific risks they pose, performing enhanced due diligence is the most important precursor to any training program, including background and integrity checks. Refinitiv, for example, provides compliance teams with enhanced due diligence reports that focus not only on the company, its owners, and its operating and litigation history, but also on key management and decision makers.

These Refinitiv reports specifically provide insight on the company and individuals' "backgrounds, track records, competencies, potential conflicts of interest, and political and criminal links," Refinitiv said. "Business conduct and reputation history are analyzed, and a thorough search is made for hidden liabilities. Additional intelligence can be gathered from industry observers."

The most important thing when it comes to establishing a third-party training program is just to start. "Sit down and develop a plan for your training program," Arvanitis says. From there, you can then ensure that it is risk-based, relevant, and impactful. Taking those steps will put the company in a much better position with enforcement authorities if problems arise than if they had not taken any steps at all. ■

How do you educate your third parties on anti-bribery and corruption?
(Select as many as apply)



SECTION 3

Identifying high-risk third parties a nuanced exercise

Determining which business partners to flag for enhanced due diligence all depends on the quality, and sources, of your data.

By Joe Mont

Information abounds on company risk; finding the right data you need for improved screenings via enhanced due diligence can be the challenge.

The Compliance Week 2019 Survey on Anti-Bribery & Corruption, conducted with Refinitiv, asked respondents what sources of data they use to identify or validate the level of third-party risk for each party of concern.

Among the 15 options for sources of data, the most frequently cited were public records (74 percent of respondents), international screening databases (68 percent), internet/social media searches (64 percent), adverse media (63 percent), and content on politically exposed persons (57 percent).

When initiating the enhanced due diligence process, a firm will also need to assess the available data and intelligence.

"Ultimately, with every third party that you're screening, you're often going to be using a questionnaire," says Kevin Bogdanov, director of market development – risk, Americas, for Refinitiv's third-party risk management business. "They want to do business with you, and so you send them a document they need to fill out. It will have information like: 'How many employees do you have? What's your annual turnover? Tell us about your business structures and processes.' "

"Then there'll also be more kind of pointed stuff around child labor. Or, 'Can you attest that you do not pay bribes to secure business?' You're relying on that information that is provided to you by that supplier and by that third party, agent, contractor, or whoever."

"However, that's obviously limited data. If I'm self-reporting risk—if I'm a third party—I may not tell you that I'm linked to a sanctioned entity. So the confluence between the data that is sourced from the third party and the data that is externally available, whether it's a sanctions watch list or any other types of data, like address media and court filings and whatever else that is going to be, what do you use to assess the level of diligence that's required—that confluence between both available self-sourced and independently verified data?"

Other upfront, factual determinations include parameters for what motivates additional financial diligence. Does the deal involve a high-risk jurisdiction? Are you working in Bulgaria or Uzbekistan or maybe parts of Asia, Africa, or the Middle East? Or, instead, are you doing a deal in New Zealand or Norway, "where it is obviously going to be a different thing," Bogdanov says.

What is the volume? Is it a couple of containers, or shiploads? What

"Ultimately, with every third party that you're screening, you're often going to be using a questionnaire. They want to do business with you, and so you send them a document they need to fill out. It will have information like: 'How many employees do you have? What's your annual turnover? Tell us about your business structures and processes.' "

Kevin Bogdanov, Director of Market Development – Risk, Americas, Refinitiv

is the monetary value? "Obviously, when you have very high volume and exposure, it's going to necessitate due diligence more often than not," says Bogdanov.

Is interpretation of public data sources a challenge when making the decision that enhanced due diligence is required? Can even usually unimpeachable public data sources be misleading or cry out for further scrutiny?

"I'll give you a silly example," Bogdanov says. "Sometimes, I myself am considered a Politically Exposed Person, albeit in the most benign way possible. My uncle is a police director in Bulgaria."

"Not that it is particularly relevant," he adds, "but it does make me a PEP, even if it is absurd that it would have any bearing on anything because I live in the U.S. and I'm not involved in anything that actually ties to police work. It is just a classic example of where, just because somebody is a PEP, it can be completely benign and completely irrelevant, or it could be highly relevant. It just depends, and more research is needed."

Why might this data be relevant? It could be meaningful if you, for example, are dealing with a large multimillion-dollar project in a high-risk part of the world—Uzbekistan or someplace like that—and in order to get the deal across the line, you need local ministerial approvals and permits to build industry infrastructure in the local network. "All of a sudden, you are dealing with PEPs who have the ability to either accept or reject the project or bid," Bogdanov says. "Now, that's a very different situation."

"What I would advise is that every organization needs to establish a risk-based approach from the onset—at the beginning of the process, before any of the screening and diligence even happens. This risk assessment will determine what types of risk matters most to them. Firms can then leverage all of the available data that they have to determine whether any of those criteria are met."

Bogdanov also suggests that businesses "have a very narrow view of what their risk threshold is."

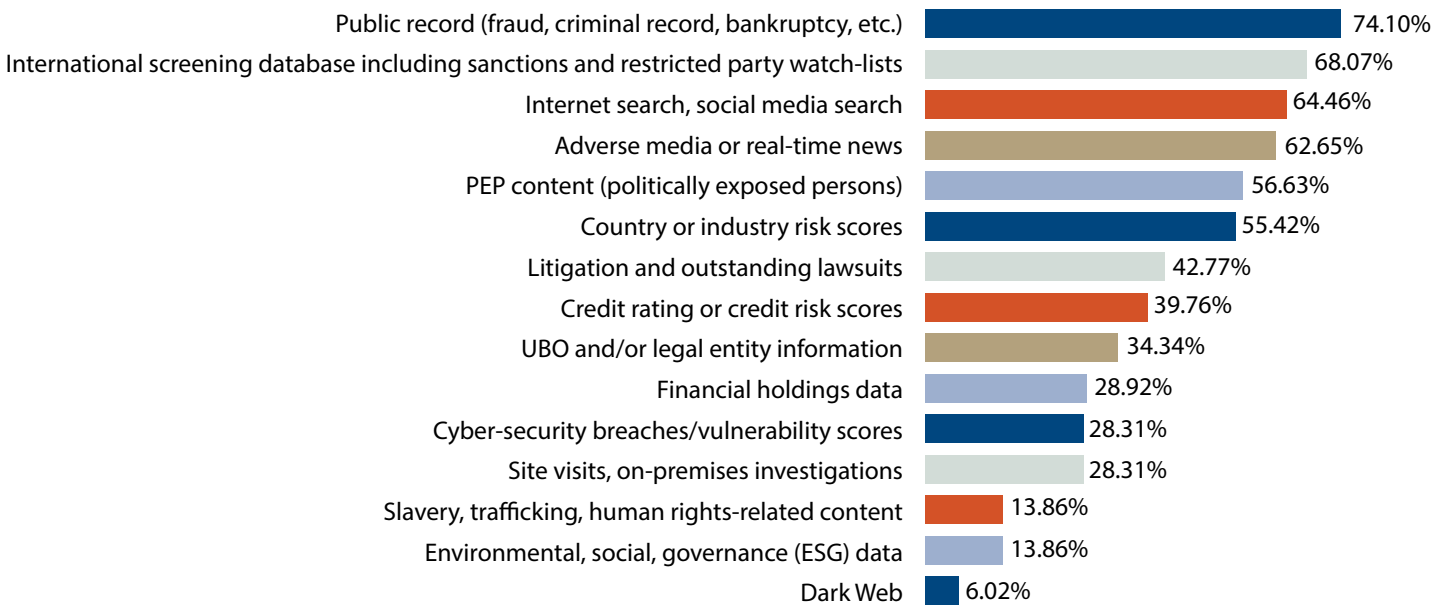
For example, there are some really good available sources of data, like Transparency International, and others to talk about bribery and corruption risk, but there are ultimately 50-plus different risk indicators.

"You could look at a country, or a place of doing business, and sort of determine what their risk of violent crime is, their risk of child labor, of corruption of money laundering, or extortion, of whatever," he says. "There are all these different indicators out there and, if you have a far more nuanced view of what types of risks happened and at what level, you can create an automated risk threshold."

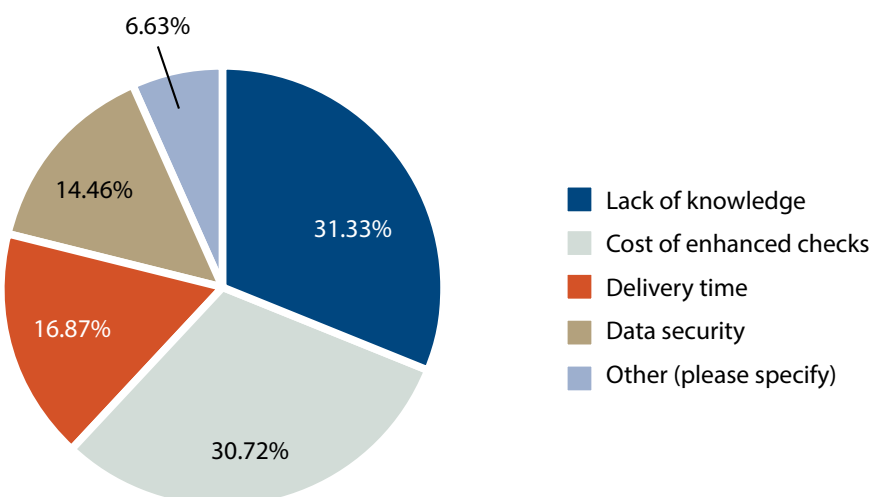
"A lot of our Western customers crave really intuitive, but really advanced, kinds of programs where they automatically create a new due diligence report. They're able to be scientific about it, and it takes the emotion out of it. We really advocate for a scientific, objective, automated, integrated threshold inside the programs, which is not that hard to do." ■

The Compliance Week 2019 Survey on Anti-Bribery & Corruption, conducted with Refinitiv, asked respondents what sources of data they use to identify or validate the level of third-party risk for each party of concern. Among the 15 options for sources of data, the most frequently cited was public records (74 percent of respondents).

What sources of data do you use to identify or validate the level of third-party risk for each party of concern? (Select all that apply)



What is the biggest challenge you face at the "enhanced due diligence" stage of the process?



SECTION 4

Dark Web grows as an investigative tool

A shady outpost of the internet is increasingly a place to search out malfeasance and ID theft.

By Joe Mont

A telling detail uncovered in the 2019 Survey on Anti-Bribery & Corruption was that about 6 percent of respondents said they extend their data searches into the "Dark Web." So what exactly is the Dark Web, and how does one use it in the due diligence process? An online Refinitiv white paper delves into it:

"This is a fundamental challenge facing everyone involved in the fast-paced world of emerging technologies and new ideas—a world where technology can be adopted for the benefit of society, but also exploited by those bent on criminal activity," it reads.

"Many would agree that the Amazon 'experience' of legally purchasing books, music, and other items brings benefits to consumers. We freely use an Amazon I.D. to log in, make transactions, keep a browsing and purchase record, and receive recommendations on other things we might want. But unbeknown to most, a similar 'storefront' model exists on the Dark Web for weapons, drugs, and stolen identities."

"There is no panacea for solving this problem, but it demonstrates the need for those who develop and protect these systems to remain one step ahead. In the same way that criminals seek to exploit technology for their purposes, if we want to tackle financial crime, or terrorism, we must develop new systems to find it, track it, and keep it out of our systems," it adds. "The core to this is identity: If we can do a better job on identity verification at point of entry, we can do a better job on the backend of transaction risk management."

That is why searching the Dark Web is so important. Most public-facing Web content is mapped on a constant basis with "spiders" that allow search giants like Google to give users nearly instant access. The Dark Web, however, was designed without a roadmap and requires specialized tools. For example, the well-known Tor browser.

The Tor Project, a non-profit, began "onion routing" in the 1990s. The Tor browser is its tool for using the internet with as much privacy as possible by routing traffic through multiple servers and decentralized networks, each with encryption.

When deployed, Tor code was released under an open software license. Its network grew to nearly a dozen volunteer nodes in the United States and Germany. Later came bridges to the Tor network to address censorship, thereby "gaining popularity among activists and those interested in privacy, although still difficult for less-technically savvy people to use," notes to an online history of the Tor Browser.

Development of a new Tor Browser made it more accessible to average-skilled internet users and activists by protecting online identities, while allowing access to otherwise blocked resources, social media, and Websites.

Those ideals, however, were corrupted. If you know where to look, all manner of illegal items are for sale, including guns, human trafficking, drugs, and stolen identities and financial information."When you look at all the peer-to-peer money movements that take place every day, including immigrants repatriating money, there are millions of small-dollar money movements going on at any given point in time. Is that a genuine worker who is simply sending money back to his family, or is that $100 going to fund criminal or even terrorist activity?"

"Determining identity is therefore a key part of risk management for any transaction," the Refinitiv white paper says. ■

> "In the same way that criminals seek to exploit technology for their purposes, if we want to tackle financial crime, or terrorism, we must develop new systems to find it, track it, and keep it out of our systems."
>
> Refinitiv white paper

Contributors

JACLYN JAEGER
EDITOR, COMPLIANCE WEEK
Jaclyn Jaeger is an editor with Compliance Week and has written over 2,000 articles on a wide variety of topics, including ethics and compliance, risk management, legal, enforcement, technology, and more. Prior to joining Compliance Week, she spent four years as a legal reporter for Lawyer's Weekly. Jaclyn attended undergraduate school at St. Joseph's College of Maine and graduate school at Emerson College, earning degrees in journalism.

DAVE LEFORT
EDITOR IN CHIEF, COMPLIANCE WEEK
Dave Lefort is an award-winning journalist with an extensive background in content management, digital strategy, and data analytics. He spent nearly two decades in digital leadership roles at The Boston Globe and ESPN.com.

KEVIN BOGDANOV
DIRECTOR OF MARKET DEVELOPMENT – RISK, AMERICAS, REFINITIV
Kevin Bogdanov is Director of Market Development, Americas for Refinitiv's Risk business. He has spent 12 years leading international teams and programs in the Enterprise Information Services, Technology, Finance, Risk and Compliance sectors. He's currently exploring how data, technology, automation and AI will disrupt and redefine the practice of KYC and third party risk compliance.

JOE MONT
STAFF WRITER, COMPLIANCE WEEK
Joe Mont has been an award-winning journalist for nearly 25 years in the Greater Boston area. A staff writer with Compliance Week, he previously covered business and personal finance for TheStreet.com, was editor-in-chief of the Bulletin Newspapers chain of publications, was co-publisher and editor of Cigar Lifestyles Magazine, is a published author, and has been a frequent guest on radio stations throughout the country.

About Compliance Week

COMPLIANCE WEEK

Compliance Week is an information service on corporate governance, risk, and compliance that features weekly electronic newsletters, a monthly print magazine, roprietary databases, industry-leading events, and a variety of interactive features and forums. Published by Wilmington Group plc, Compliance Week reaches more than 26,000 compliance, ethics, financial, legal, audit and risk executives. It is based in Boston, Mass.

About the sponsor

REFINITIV™

DATA IS JUST
THE BEGINNING

One of the world's largest providers of financial markets data and infrastructure, and serving more than 40,000 institutions in over 190 countries, we deliver trusted risk management solutions that encompass regulatory change, anti-bribery and corruption, third party and supply chain risk, anti-money laundering, financial crime, KYC, and enterprise GRC management.

To help mitigate risk, Refinitiv provides an end-to-end third party risk management solution to take your internal processes from initial screening and due diligence through on-boarding and monitoring. At our core is a unique open ecosystem of expert partners and curated products that uncovers opportunity and drives change.

The possibilities? Endless. A dynamic combination of data, insights, technology, and news means you can access solutions for every challenge, including a breadth of applications, tools, and content – all supported by human expertise. To learn more, visit refinitiv.com.

REFINITIV
DATA IS JUST THE BEGINNING.

At Refinitiv, we have a bold vision for the future. Formerly the Financial and Risk business of Thomson Reuters, we are a new company built on a unique open platform, high performance products, and world-class data.

Refinitiv Risk Management solutions provide the data, technologies and expertise to manage risk and regulation. Leveraging data and tools like World-Check® and Enhanced Due Diligence, we connect you to greater opportunity, enabling your organization to overcome regulatory challenges and avoid reputational and financial risk.

World-Check • Enhanced Due Diligence • KYC as a Service • Connected Risk

refinitiv.com

REFINITIV™

DATA IS JUST
THE BEGINNING