Kroll

COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

2014 Anti-Bribery and Corruption Benchmarking Report

Untangling the Web of Risk and Compliance

A collaboration between Kroll and Compliance Week

Table of Contents

**"Oh! what a tangled web we weave
When first we practise to deceive!"**

Sir Walter Scott

It may start with something seemingly small. It may begin as a full-blown crisis. No matter how the issue comes to light, the chief compliance officer is charged with untangling a mess that could get much worse if not handled properly. The design theme for this year's Anti-Bribery and Corruption Benchmarking Report reflects these risks through images that suggest the complex nature of the topic. The nets, hooks and webs are not only a reminder of how easily things can go wrong, but also how these traps can be avoided altogether with the right people, preparation and planning.

Welcome to the 2014 Anti-Bribery and Corruption Benchmarking Report ("ABC Report"), a joint effort between Kroll and Compliance Week. Here we strive to give compliance professionals insight into the most important issue they face: effective programs to root out bribery and corruption. The modern global enterprise faces a more demanding regulatory environment than ever before, as well as more risks of bribery and corruption than ever before — and compliance officers must address both of those concerns amid a relentless pressure to be as cost-effective and efficient as possible. The goal of this report is to help compliance officers accomplish exactly that.

First launched in 2011, the ABC Report aims to give compliance officers a comprehensive view of the "ABC" (anti-bribery and corruption) risks they have, the resources they have to fight them, and how those resources are implemented into compliance programs. We began this specific report in the depths of winter, creating a 30-question survey that explored a wide range of issues confronting ABC programs today. Those 30 questions were grouped into three broad categories: the resources and authority compliance officers have to address ABC risks; the nature of what those risks are; and the due diligence and compliance programs businesses put in place to fight them. We also included two free-response questions to let survey-takers express their thoughts more directly.

We then asked compliance executives worldwide to take the Anti-Bribery and Corruption Benchmarking survey. Nearly 200 responded, and participants hailed from all manner of industry. Their companies had median annual revenue of $3.5 billion and on average more than 9,600 employees — in other words, the true voices

of modern, global business. Their answers gave us the raw material to understand ABC risks and compliance programs today, and we're grateful for their invaluable input.

While we started with three categories of questions, we actually ended up with four categories of insights: risks, third parties, due diligence efforts, and program effectiveness. In this supplement, you'll find an executive summary of the results on pages 6–9 and then snapshots of select findings from each of those four categories, plus more context on our methodology and how you can put these survey findings to good use at your own organization.

We hope you find the information here useful and that it can serve as a guidepost for your efforts to understand how corporate compliance works best in your company.

Matt Kelly, Editor and Publisher, Compliance Week
Lonnie Keene, Managing Director, Compliance, Kroll

"It's no longer just implementing the individual elements that make up a program, but figuring out how to make it all work together, and how to make it all work together as a single program that's effective."

Lonnie Keene
Managing Director, Kroll

Executive Summary

Foremost, the 2014 Anti-Bribery and Corruption Benchmarking Report ("ABC Report") shows that compliance departments still struggle to understand and tame several key corruption risks. Compliance officers' understanding of how their anti-corruption programs should work is fairly widespread; one can certainly say many "standard" anti-corruption compliance practices have emerged and been adopted. Still, as we've seen in prior years:

- Large U.S. corporations lead the way in anti-corruption programs and worry more about bribery risks, while smaller and overseas businesses trail behind.
- Third parties continue to vex compliance officers; in 2014, the percentage of respondents who said they don't train their third parties on anti-corruption actually went up.
- Due diligence at the beginning of a business relationship is strong, but monitoring anti-corruption efforts on a continuing basis is weak.

And for the first time, this year the ABC Report also asked compliance officers exactly what types of misconduct qualify as "corruption" that they are responsible for addressing. To no surprise, bribery topped the list, cited by 95 percent of respondents. Following behind it were bid-rigging, money laundering and price-fixing. We also asked about the chief compliance officer's (CCO's) role in cyber security risk: 44 percent said the CCO is only responsible for breach disclosure after a privacy breach of some kind, and 31 percent said the CCO plays no role in cyber security or breach disclosure at all.

To understand the CCO's delicate position today, we must consider all these circumstances together — that even while several elements of an effective compliance program still pose problems for many CCOs (risk assessments, third parties, monitoring), the types of risks their programs must address are proliferating (money laundering, bid-rigging, data security).

That does not portend easy times for compliance officers in the next several years. It does, however, help frame the right questions a CCO can ask about an organization's program and how to make it more effective.

RISKS

For the second year in a row, large U.S. corporations were much more likely to say they expect bribery and corruption risks to increase than smaller or overseas corporations do. As a whole, 51 percent of respondents said they expect more such risks in the next two to three years — as did 57 percent of U.S. companies, and 57 percent of large companies ($5 billion or more in annual revenue). But only 37 percent of overseas businesses, and 46 percent of smaller companies, expect their corruption risks to keep rising. For both of the latter groups, a much larger number expect their corruption risks to remain relatively unchanged.

One question compliance officers can ask, then, is whether their assessment of bribery risks is accurate. The "risk perception gap" between large and small, or U.S. and overseas, does exist, and an erroneous understanding of one's risk profile can have dire consequences.

Compliance officers are less involved — or perhaps, their proper role is less clear — in managing cyber security risk. The most common arrangement, cited by 44 percent of respondents, is that the CCO is responsible for privacy compliance and breach disclosure after an incident, but not for cyber security before one. Thirty-one percent of respondents said the CCO has no role in cyber security nor in privacy breach disclosure. Conversely, 22.5 percent said the CCO is responsible for both data security and breach disclosure. In other words, 75 percent of compliance officers are not involved in managing cyber security risk.

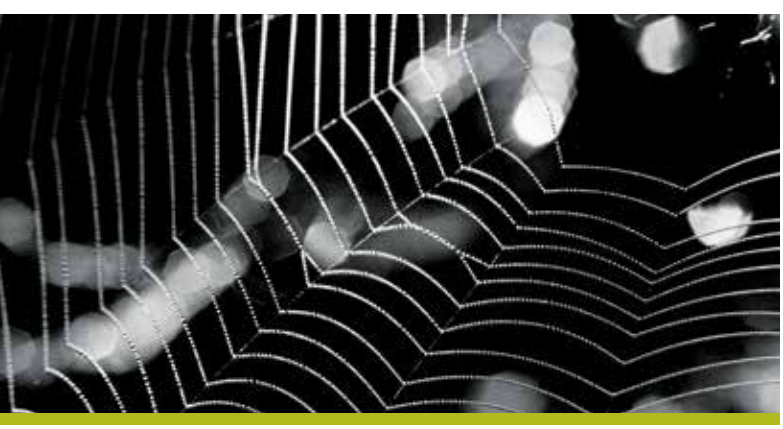
THIRD PARTIES

Taming third-party risks continues to be a major weakness for anti-corruption programs, and the problem may well be getting worse. Survey respondents this year reported an average of 3,868 third parties, yet 58 percent say they never train third parties on anti-corruption efforts. That number is higher than last year's ABC Report, when 47 percent said they do not educate third parties on anti-corruption policies.

Tellingly, however, the number of companies that conduct due diligence on third parties has increased, from 87 percent in 2013 to 97 percent this year — which suggests that companies do now grasp the importance of performing due diligence and have the processes in place to do so. That next step of training third parties (which can indeed be expensive) is where compliance programs start to falter.

Third-party risks do hinge on several factors, such as the number of third parties one has or the corruption environments where they are. Another question that CCOs can ask themselves, then, is how the need for the services provided by their third parties matches up with the risk they pose to their companies.

The 42 percent of respondents who do educate third parties tend to work on a sliding scale: the more time and energy a certain technique requires, the less often it's used. Most common were including an anti-bribery statement in the company's Code of Conduct (70 percent) or having the third party certify its awareness of anti-corruption efforts in contracts (59 percent). Least common were in-person training (42 percent) and posting printed materials (45 percent).



DUE DILIGENCE

This is a bright spot in the 2014 ABC Report. In addition to the 97 percent of respondents who perform due diligence on third parties (cited above), 92 percent say they perform at least some due diligence on merger and acquisition targets to identify possible corruption risks before a deal is done. What's more, 74 percent say they start by investigating the target company's management team — which is where the most serious corruption risks typically hide.

Due diligence on a target company's third parties fell off sharply: only 54 percent also performed due diligence on a target's agents, 52 percent on its distributors, 50 percent on its consultants, and 46 percent on its suppliers. And as we will see elsewhere in this report, larger companies were much more likely than smaller ones to perform due diligence on a target's third parties.

Those more distant third parties are another weak spot in the supply chain. Consider, for example, the Rana Plaza factory collapse in Bangladesh that killed more than 1,100 workers. Western retailers go to great lengths to assure the public that their contractors in emerging markets are not unsafe sweatshops — yet numerous samples of Western brands' clothing were found at Rana, which had subcontracted work from those ostensibly safe first contractors. A question for CCOs here, then, is to ask how well their due diligence procedures can peer down the supply chain into the ecosystem of third parties, M&A targets and the like.

EFFECTIVENESS

Seventy percent of respondents rated their policies for domestic employees as effective or very effective — and larger companies were more bullish about their domestic employees than smaller ones (77 percent to 61 percent, respectively). That statistic edged downward for confidence in training overseas employees, to 66 percent, driven by considerably fewer companies saying they were very confident in their training of overseas workers.

Compliance officers were more confident in their ability to vet third parties at the start of a relationship, and less confident in monitoring third parties once that onboarding examination had passed. Fifty-seven percent of respondents rated their vetting procedures as effective or very effective. Then the numbers marched downward for monitoring compliance after a relationship starts (43.3 percent), auditing compliance of third parties (33.2 percent), and training third parties on anti-bribery and corruption procedures (30 percent).

Effective compliance programs can identify corruption risks when the CCO is not specifically hunting for them. That may come from strong training in a speak-up culture, or strong audits of third parties, or any number of other techniques. The key question here is to ask what metrics and corruption risk indicators match the risks you believe you have, and how your compliance program can implement them.

"Every compliance officer needs to decide whether it's time for them to be Captain Kirk and boldly go into cyber..."

Alan Brill
Senior Managing Director, Kroll

Risk

For the second year in a row, large U.S. corporations say they expect bribery and corruption risks to increase considerably more than smaller or overseas corporations do. Given the globalized nature of modern business — with more regulatory scrutiny, from more regulators and the "extended enterprise" extending to include ever more third parties — this raises the same question as last year: Do smaller or non-U.S. businesses truly have fewer corruption risks, or do they misunderstand the risk profile they have?

The numbers show a clear gulf. As a whole, 51 percent of respondents said they expect more such risks in the next two to three years; 57 percent of U.S. companies, and 57 percent of large companies ($5 billion or more in annual revenue) say the same. But only 37 percent of overseas businesses, and 46 percent of smaller companies, expect their corruption risks to keep rising. For both of the latter groups, a much larger number expect their corruption risks to remain relatively unchanged.

Melvin Glapion, a managing director at Kroll, says the divergence reflects the reality that U.S. regulators still mostly pursue bigger game when prosecuting cases under the Foreign Corrupt Practices Act ("FCPA"), although eventually they will set their sights lower. "Smaller and non-U.S. companies feel under less of a threat, but it's only a matter of time before U.S. and local authorities expand focus to make examples of these companies," he says. "At the moment, however, government resources are limited, so these companies feel somewhat less threatened."

This year the 2014 ABC Report also tried to define the types of corruption that compliance officers worry about. To no surprise, bribery was by far the primary concern, cited by 95 percent of respondents. Other common corruption risks were bid-rigging (65 percent), money laundering (62.5 percent) and price-fixing (60 percent). Even conflict minerals and human trafficking made the list, at 24 percent and 20 percent, respectively.

"I think the evolution will be to what extent can compliance be baked into functional areas, and the compliance officer will become the coordinator, or the record-keeper, or the reporter," says Alan Brill, a senior managing director for Kroll. "Maybe what we're evolving to is the compliance officer becoming more like an internal auditor. But certainly the role of the compliance officer has evolved so much that if you put a compliance officer from 15 years ago in a time machine, he or she wouldn't know how to respond today."

One of the most pressing issues for compliance officers today — and for CEOs, boards, regulators, and the public, for that matter — is cyber security risk. Thirty-one percent of respondents said the CCO has no role whatsoever in cyber security or in privacy or breach disclosure. Conversely, 22.5 percent said the CCO is responsible for both data security and breach disclosure.

The most common scenario, however (cited by 44 percent of respondents), was a split decision: the CCO is responsible for privacy and breach disclosure after an incident, but not for cyber security before one.

"Every compliance officer needs to decide whether it's time for them to be Captain Kirk and boldly go into cyber, and to do it by forging a partnership with the IT director, with the general counsel, with the internal auditor — so that the cyber elements of compliance are just the everyday part of your work," Brill says. "The best solution is when this is just recognized as part of what compliance officers do."

Most companies will not be able to add a full-time "cyber-person" to the compliance staff, Brill says. But compliance officers should have a strong enough grasp of the issues to know when they should be involved in a problem — and, he stresses, other parts of the corporate enterprise need to recognize that compliance has a role to play from the beginning.

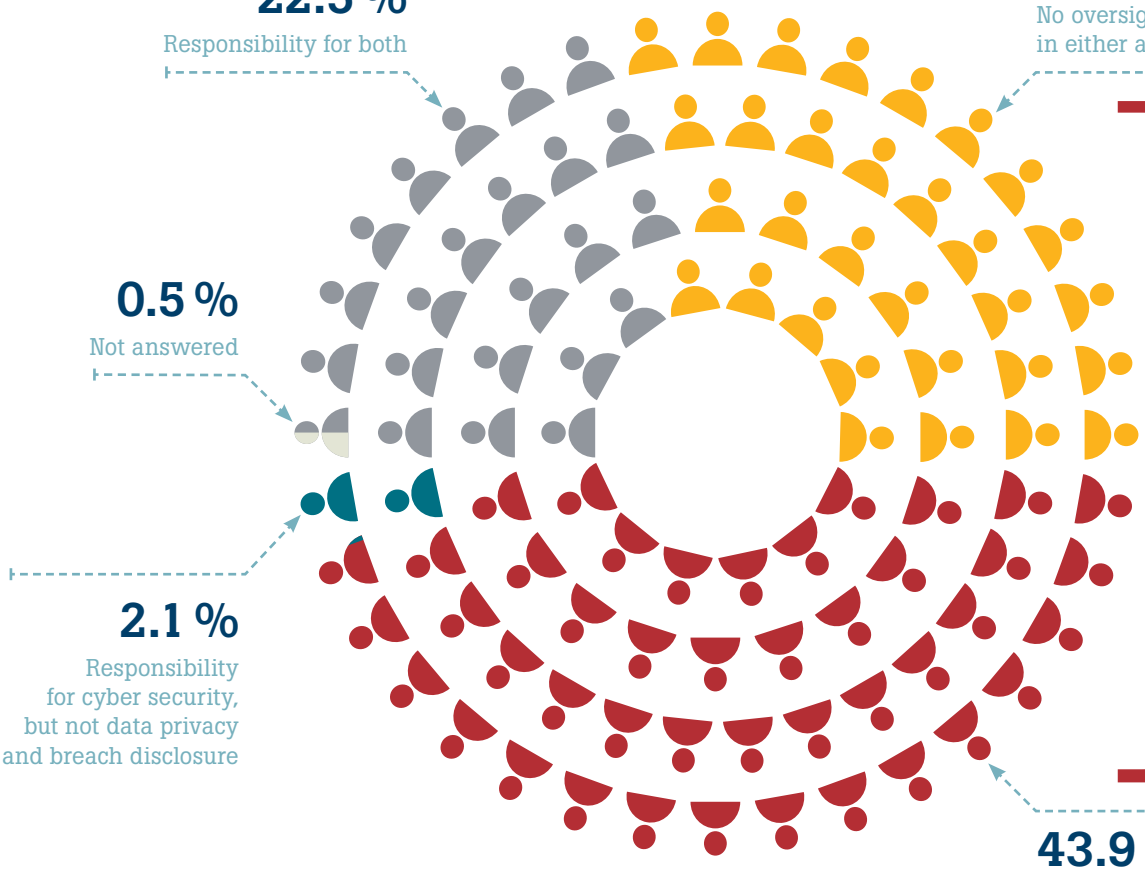
"There is an expectation that a company will have commercially reasonable levels of cyber security. That expectation, where it isn't met, can certainly lead to compliance issues," Brill says.

Even worse, the risks from a cyber security lapse can often involve hefty penalties or sanctions, civil litigation, and damage to a company's reputation — all of which are bound to draw the ire of CEOs and audit committees caught by surprise. This spring's Heartbleed bug (a mistake in e-commerce encryption codes that hackers learned how to exploit) is a perfect example: it affected thousands of companies in an area nobody expected. "I think it's not just fair, but very realistic, to say that a cyber-crisis can occur at any time and can occur from things that you would believe weren't a risk," Brill says.

Thus Brill recommends that compliance officers hone their "incident response plans" over and over. Companies need to know where their data is stored, the specifics of state and country disclosure requirements, and what outside forensic or response help would be needed in the event of a breach, and have all the resources ready to go if a problem occurs. They cannot afford to waste time reviewing contracts for outside resources when the clock is ticking to respond, Brill says.

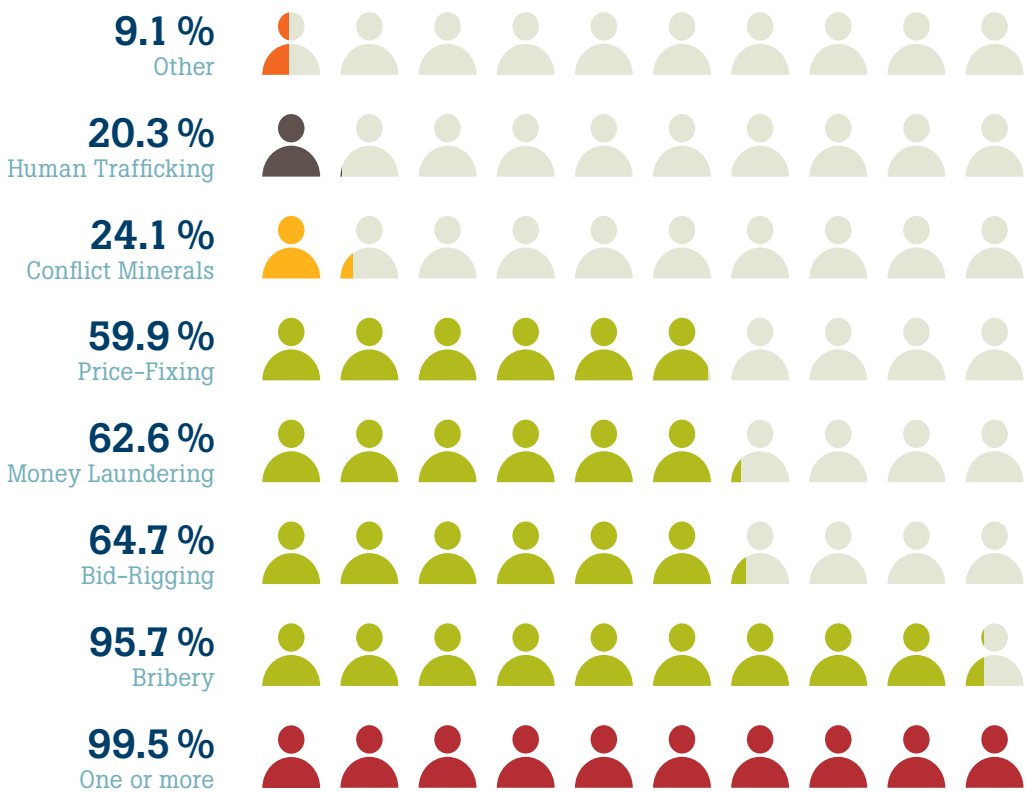
"For those who don't think about and plan for this, you can suddenly be in the middle of a regulatory crapshoot — not particularly where you want to be in the middle of a crisis," he says.

What is the chief compliance officer's responsibility for data privacy laws and cyber security?



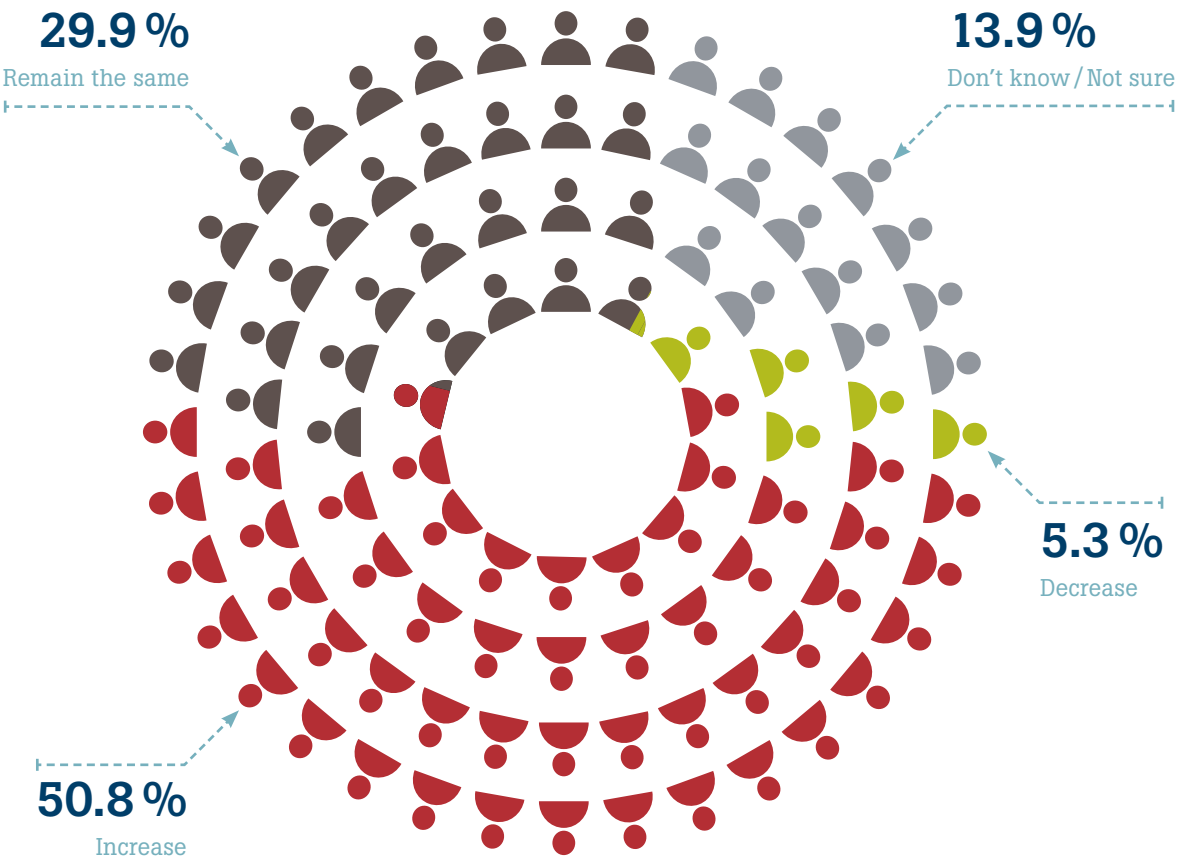
SURVEY BASED ON **187** RESPONDENTS

Exactly what types of misconduct does your company label "corruption" that the chief compliance officer is responsible for policing?



SURVEY BASED ON **187** RESPONDENTS

Do you anticipate the bribery and corruption risks to your company will increase, remain the same, or decrease over the next two to three years?



"Yes, I expect my bribery and corruption risks to increase in the next two to three years…"

Large companies: 57 percent
Small companies: 46 percent
U.S. companies: 57 percent
Overseas companies: 37 percent
Overall: 51 percent

Third Parties

Third parties continue to be the bane of anti-corruption programs. Survey respondents this year reported an average of 3,868 third parties, and yet 58 percent of respondents said they never train third parties on anti-corruption efforts. That number is even higher than reported in last year's ABC Report, when 47 percent of respondents said they do not educate third parties on anti-corruption policies.

Lonnie Keene, managing director for Kroll's compliance practice in New York, minces no words about that figure: "It's amazing in this day and age, given the importance and the focus on anti-bribery and anti-corruption, that 58.3 percent would say they never train their third parties." He noted that of those who do train their third parties, more than a quarter fail to do so in local languages.

Interestingly, the number of companies that report conducting due diligence on third parties has increased, from 87 percent in 2013 to 97 percent this year.

Melvin Glapion, managing director at Kroll, says that discrepancy suggests a fundamental problem. "What I'm seeing [in the survey results] is that people give good, very positive political statements about what they're doing, but if you actually scratch a little bit harder, what you see is that the follow-through doesn't support it," Glapion says. "Everybody has some form of anti-bribery policy in place. What they're not doing is educating their third parties, which is where most of the risk is."

The 42 percent of respondents who do educate third parties tend to work on a sliding scale: the more time and energy a certain technique requires, the less often it's used. Most common were including an anti-bribery statement in the company's Code of Conduct (70 percent) or having the third party certify its awareness of anti-corruption efforts in contracts (59 percent). Least common were in-person training (42 percent) and posting printed materials (45 percent).

Companies are much more confident in their procedures for vetting third parties than they are in their processes to monitor and audit those third parties on an ongoing basis. That comes as no surprise to Glapion, who senses a "vet it and forget it" mentality where companies rarely revisit their existing third parties.

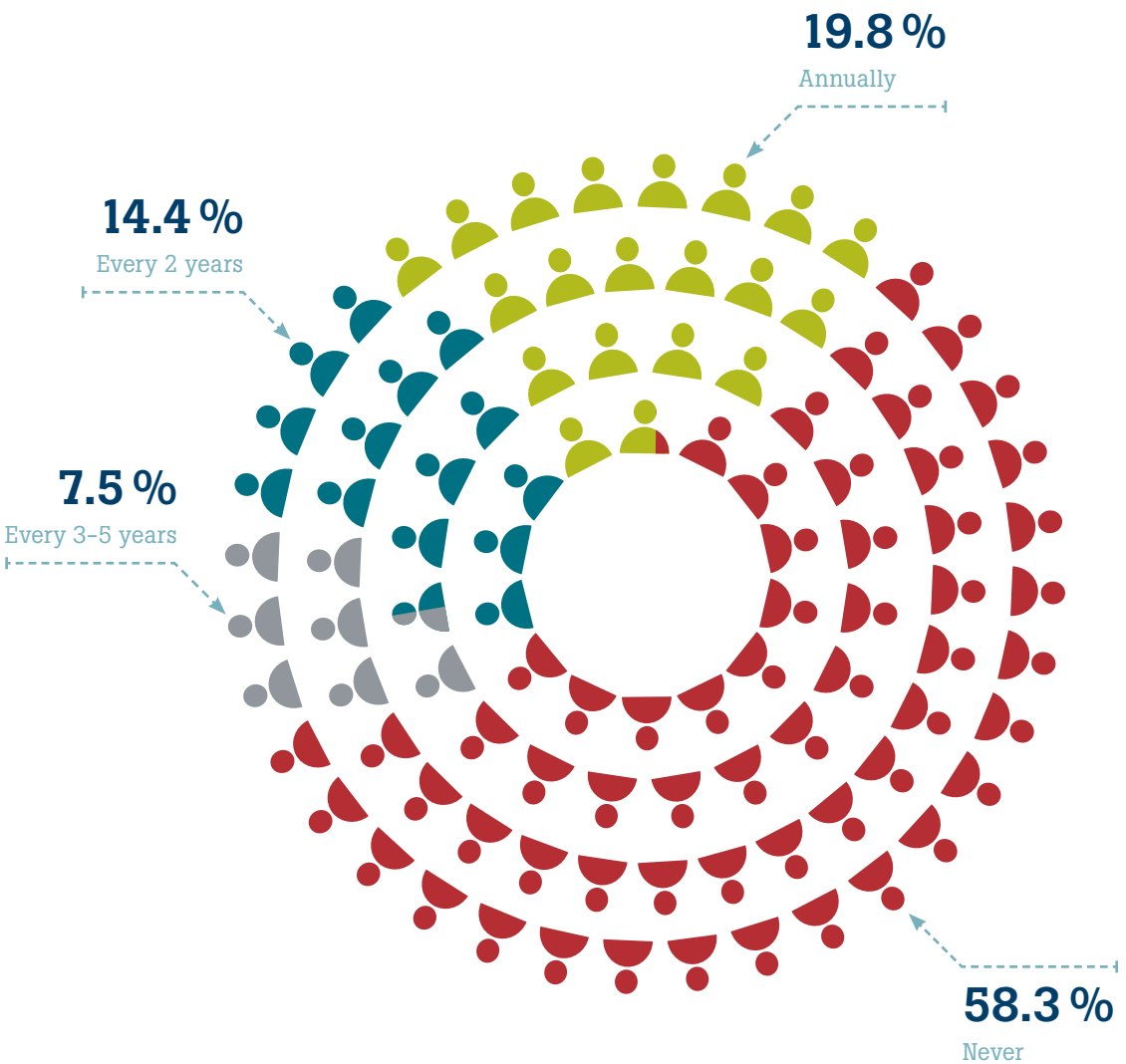
Glapion recommends that companies group their third parties into low-, medium-, and high-risk partners, and re-evaluate all of them on a four-year cycle. Companies should then review that data to find where the red flags arose and how those were handled. For example, did you reject a partner because of the red flag, or use it as an opportunity to reduce the company's exposure through conversations and training with that errant third party?

"Most people will think the gold standard is adjusting the due diligence to the risk," he says. "It's more than just the risk flexing; it's also how you go about sharpening the saw, and improving the processes and measuring that information that's coming back to you."

Survey respondents cited all the obvious reasons for taking a pass on a third party: rumors of paying bribes without actual proof (77 percent), history of litigation (64 percent), and politically exposed persons working at the third party (60 percent). But Glapion pointed to another factor that should also raise concerns — systemic "hygiene" issues, like widespread labor force problems or allegations of poor environmental standards. While those don't qualify as corruption or bribery, they may point to someone "unsavory" and better to avoid.

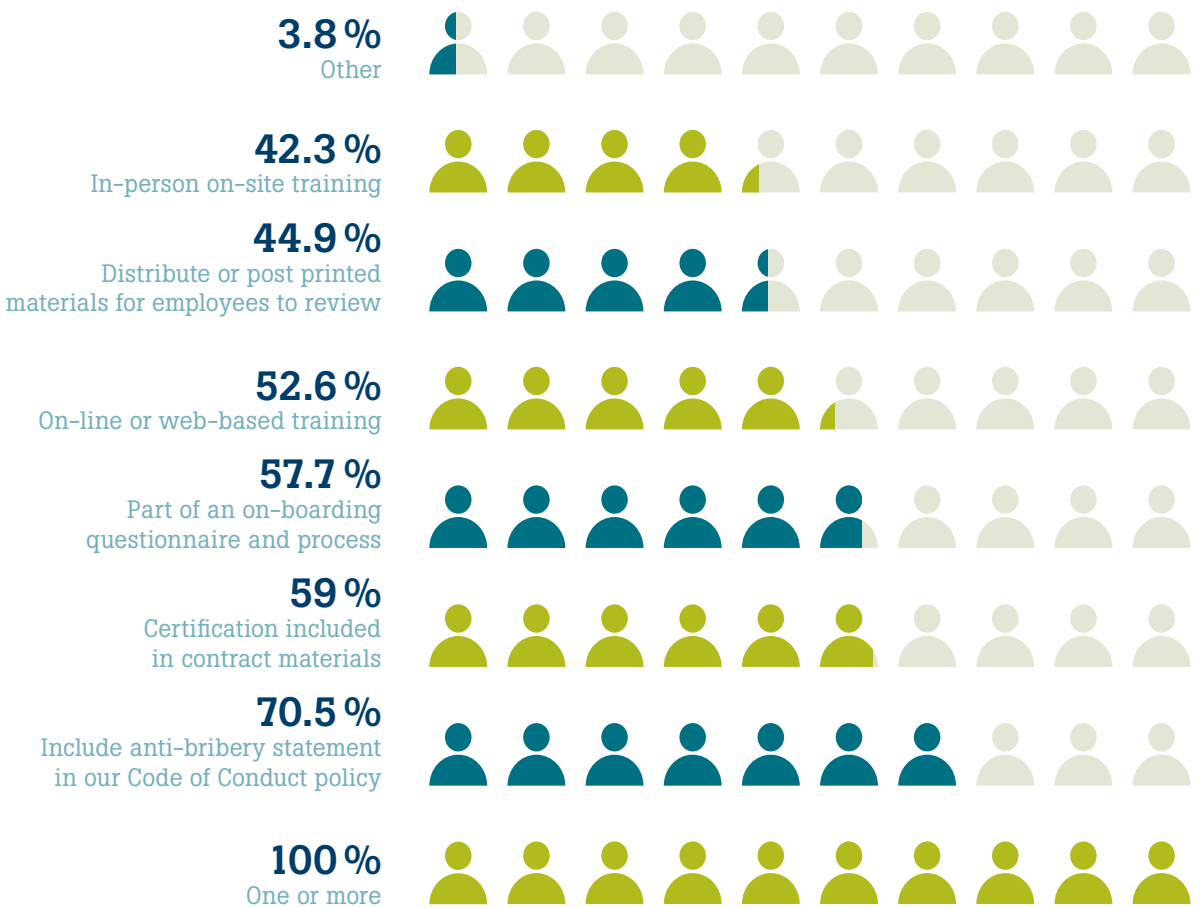
"Oftentimes what you find is when someone is cutting corners on environmental issues or labor issues and it's significant, that often means that they're cutting corners elsewhere," Glapion says. "Usually one of the places they're cutting corners is also in corruption and bribery."

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



SURVEY BASED ON **187** RESPONDENTS

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



SURVEY BASED ON **187** RESPONDENTS

Effectiveness

Compliance officers' confidence in their anti-corruption programs follows a natural progression: the closer the employee is to main headquarters, the more confident the CCO is that the anti-corruption message is heard and absorbed. The farther away the employee, the less confident. When third parties are involved, confidence in the effectiveness of the program drops even more.

Fully 70 percent of respondents rated their policies for domestic employees as effective or very effective — and larger companies were more bullish about their domestic employees than smaller ones (77 percent to 61 percent, respectively). That statistic edged downward for confidence in training overseas employees, to 66 percent, driven by considerably fewer companies saying they were very confident in their training of overseas workers.

Third parties followed a similar pattern: compliance officers were more confident in their ability to vet third parties at the start of a relationship, less confident in monitoring third parties once that close-up examination had passed. Fifty-seven percent of respondents rated their vetting procedures as effective or very effective. Then the numbers marched steadily downward for monitoring compliance after a relationship starts (43.3 percent), auditing compliance of third parties (33.2 percent), and training third parties on anti-bribery and corruption procedures (30 percent). In the case of audits of third parties for compliance, nearly one-third of respondents rated their procedures as ineffective.

Melvin Glapion, Kroll managing director, says the results make sense given that most companies front-load their energy and money into vetting a third party, with much less spent on following up for continued compliance.

"There isn't that process of saying, 'OK, how did we do this year? Let's go back and talk to people about what's happened, or let's go and audit some of the companies that either we reviewed three years ago or have been third parties of ours for a long period of time'," he says.

The ideal is a system that requires periodic re-evaluation of all third parties, depending on the level of risk each one presents to the company. "And a small sliver of those should be audited," Glapion adds.

At what cost? Glapion estimates that a billion-dollar company with 3,000 third parties should spend $1 million to $2 million annually to put all third parties on a four-year review cycle. Partners classified as high-risk would be evaluated more frequently than lower-risk counterparts, and compliance officers should identify enough red flags to move partners between categories as warranted, he says.

Glapion admits that spending so much to monitor existing relationships may be a hard sell. On the other hand, he argues, the investment pales in comparison to regulatory fines that can hit hundreds of millions should a bribery offense go undiscovered. That discussion of how much to invest versus how much to risk should take place at the board level, he says.

A related statistic: 48.7 percent of respondents said they somehow automate part of their anti-corruption program, while 51.3 percent do not. To no surprise, larger companies were much more likely to use automation (63.4 percent) than smaller ones (31.4 percent).

Kroll managing director Lonnie Keene points to the lack of technology as one possible reason why so many companies do not train their third parties — CCOs lack the IT systems to let them manage a far-flung network of third parties in a cost-effective way. Larger companies may be leading the charge because they have the global networks that need managing and the resources to do it.

"I think this is a key part of the next generation of anti-corruption program design," Keene says. "It's no longer just implementing the individual elements that make up a program, but figuring out how to make it all work together, and how to make it all work together as a single program that's effective."

How effective do you believe your company's protocols and procedures are for…?

“Everybody has some form of anti-bribery policy in place. What they’re not doing is educating their third parties, which is where most of the risk is.”

Melvin Glapion
Managing Director, Kroll

Due Diligence

Due diligence continues to be an area where compliance procedures are somewhat weak, even as compliance officers know how important the task is.

The good news is that almost all respondents (92 percent) said they perform at least some due diligence on merger and acquisition targets to root out possible corruption risks before a deal is done. Investigating the target company's management team was the most common exercise, reported by 74 percent of respondents. Then the numbers fell off sharply: only 54 percent also performed due diligence on a target's agents, 52 percent on its distributors, 50 percent on its consultants, and 46 percent on its suppliers. And as seen elsewhere in this report, larger companies were much more likely to perform due diligence on a target's third parties than smaller ones.

Lonnie Keene, managing director for Kroll, says companies need to make sure they perform adequate FCPA due diligence of the target company's third-party relationships prior to an acquisition or a merger. If compliance can't reach those third parties directly before an acquisition or merger, there are other tools, he says. Compliance officers should look at the target company's own anti-bribery and corruption policies and procedures relating to its coverage of third parties, the target's due diligence program for its third-party relationships, and its third-party payment arrangements.

If a compliance department doesn't do enough digging into an M&A target's key relationships, "the company leaves itself open to a fair bit of exposure," Keene says. That's important not just for successor liability issues, he adds, but also to ensure the acquiring company's systems are robust enough to handle and integrate the new company's network of third parties.

The U.S. Department of Justice and the Securities and Exchange Commission ("SEC") have declined to sanction companies that uncovered corruption problems during due diligence, disclosed those problems voluntarily, and worked to mitigate those issues. So taking initiative and knowing what risks the company is inheriting are key. Keene says pleading ignorance "is no excuse."

Keene has encountered scenarios in which the compliance unit is brought on late in the M&A process, after the acquisition decision has been made — and then compliance must scramble to do what it can to assess the target. But the most recent Justice Department and SEC guidance suggests that even in those situations when pre-acquisition due diligence is not possible, the regulators will look instead for post-acquisition due diligence and integration into the company's ABC program, Keene says.

"What I have seen are situations where there isn't sufficient planning pre-closure of the transaction for the integration of the new business into the acquired company," he says. "That takes a lot of planning and work that sometimes doesn't happen."

Closer to corporate headquarters, Keene is also surprised that 16 percent of respondents admit they never conduct an enterprise-wide anti-bribery and corruption risk assessment of their own. "That's still quite high, and a bit surprising given all the emphasis on creating a risk-based compliance program in regulatory guidance and other anti-bribery and corruption enforcement actions," Keene says. Without that fundamental effort to figure out what risks a company faces, building an effective compliance program to address those risks becomes much more difficult.

Which factors would influence your decision not to work with a particular third party?

55.1 %
While the third party is well-known in the region, it is not known to perform the work it would be doing for us

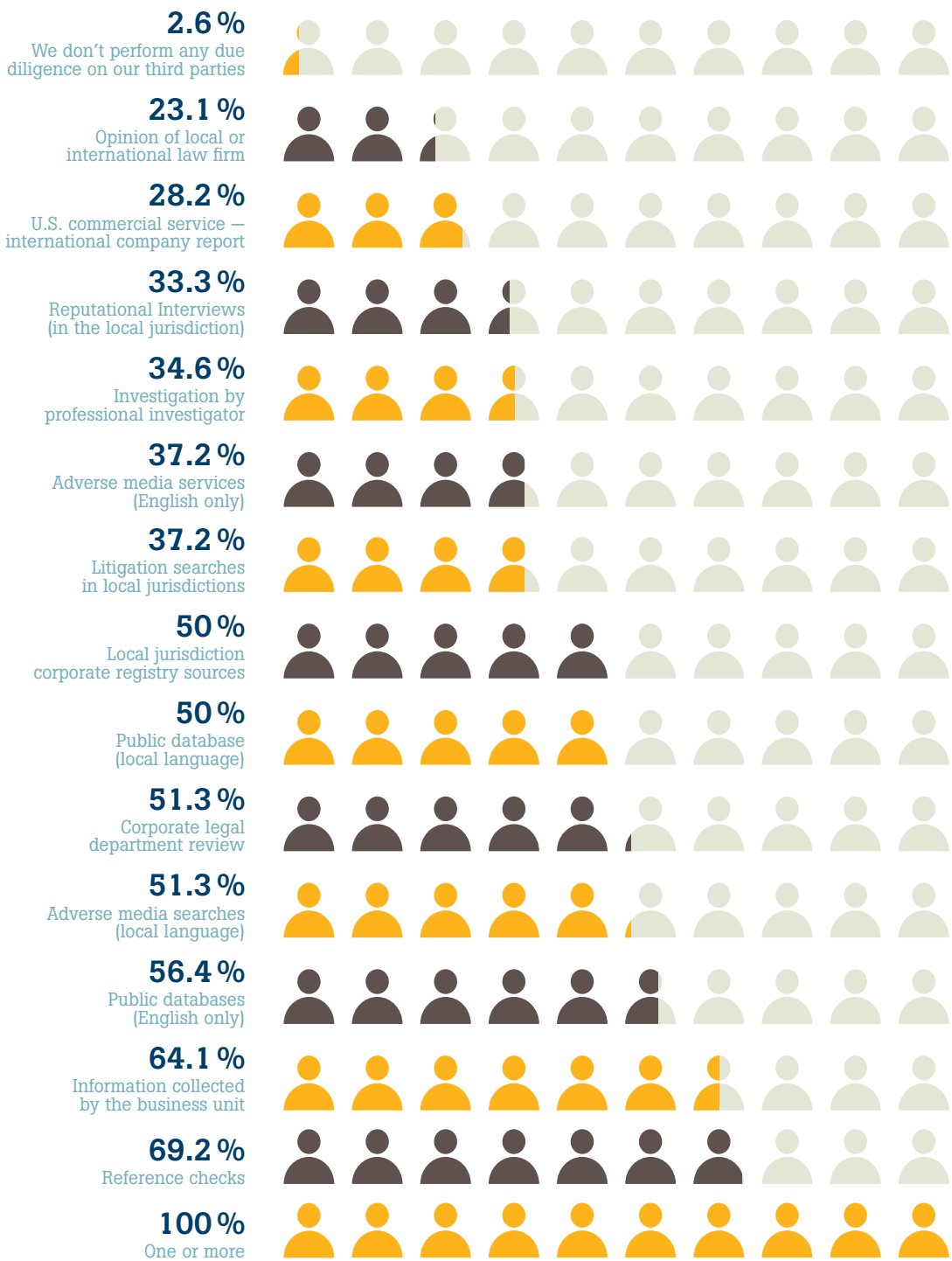
59.9 %
The third party is a politically exposed person

64.2 %
A history of litigation

77 %
Allegations/rumors of paying bribes in the third party's background, but no proof

97.9 %
One or more

What does your third-party due diligence include?



What Compliance Officers Say

How has the compliance function's focus changed at your company in the last 12 months?

"Little change in the last 12 months. Things changed significantly five years ago and then again when the UK Bribery Act came into force, that's all."

"We just completed our annual self-assessment. We're moving to more preventative controls rather than relying on internal audit as part of the control structure."

"We've dramatically reduced the number of vendors and suppliers we're working with."

"Due to the increased regulatory focus, there has been more work in regards to all aspects of financial crime. Due to the increased regulatory focus, I feel it's easier as a compliance person to get support."

"We have additional focus on distributor diligence, management, and oversight. Also additional focus on travel agencies and other third-party intermediaries working on behalf of the organization."

"I don't know of any changes."

How does the trend toward globally stronger enforcement of anti-bribery law affect your company's plans for overseas expansion?

"As a company committed to clean business, we find this very useful. We're happy that various governments across the world are introducing or strengthening their laws in the area of anti-bribery and corruption."

"It has become a factor to consider, but no negative impact."

"It won't slow anything down — but it does create leverage for additional compliance resources."

"It doesn't; expanding globally is part of our strategic plan. It's up to the compliance function to keep the company out of harm's way."

"We've slowed down expansion."

"It has made the issue more transparent, making due diligence and establishing processes easier in some of these emerging markets."

Methodology

The Compliance Week–Kroll Anti-Bribery and Corruption Benchmarking survey was drafted by senior Compliance Week editors and Kroll partners in January, and then pushed out to an audience of senior-level corporate compliance officers worldwide from Jan. 21 to Feb. 28.

The survey produced 197 responses. Any submission where the respondent's title was not directly related to corporate activities ("partner" or "administrative assistant," for example) was excluded from the data analysis. The result was 187 qualified responses from senior-level executives working in ethics, compliance or anti-corruption somehow. Of those 187 respondents, 26.2 percent held the title of chief ethics and compliance officer, followed by director of FCPA compliance (9.6 percent) and chief audit executive (9.6 percent). A wide range of other titles then trailed behind, all of them somehow related to compliance or anti-corruption activities.

The survey also went to a wide range of industries. Of the 187 qualified responses, the single largest industry group was financial services (15 percent), followed by industrial manufacturing (10.7 percent) and insurance (5.9 percent). Several dozen industries were represented in the data pool.

Median revenue of the 187 qualified respondents was $3.53 billion; median worldwide employee headcount was 9,630.

This was a self-reported survey from Compliance Week's audience of ethics and compliance professionals, and Compliance Week did not attempt to verify or audit the data reported by survey-takers.

About

Kroll is the leading global provider of risk solutions. For over 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations, and security through a wide range of investigations, due diligence and compliance, cyber security, physical and operational security, and data and information management services. Headquartered in New York with more than 55 offices across 26 countries, Kroll has a multidisciplinary team of nearly 2,300 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals.

NEW YORK

Lonnie Keene
Managing Director
T: +1 212.833.3254
lkeene@kroll.com

Greg Hoffman
Head of Sales and Marketing
T: +1 212.833.3208
ghoffman@kroll.com

HONG KONG

David Liu
Managing Director
T: +852 2884.7707
dliu@kroll.com

Rob Gho
Associate Managing Director
T: +65 6645.4950
rob.gho@kroll.com

LONDON

Grace Churchill
Head of Compliance Sales, EMEA
T: +44 20 7029.5136
gchurchill@kroll.com

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

USA

Matt Kelly
Editor and Publisher
Compliance Week
T: +1 888.519.9200
mkelly@complianceweek.com

Kroll®

Supposing is good, but finding out is better

Mark Twain

One of the greatest challenges in business is carving out time to find the right information. Kroll, the market leader for due diligence and compliance solutions, can help. Legal and compliance professionals in the world's top companies and financial institutions count on us to deliver high-quality services that enable them to focus on their most important and immediate challenges. With an unmatched global footprint, robust in-house language capabilities and flexible technology tools, Kroll calls on over 40 years of experience to provide clients with the confidence to make informed decisions and seize rewarding opportunities.

Our services include:

SCREENING AND DUE DILIGENCE	TRANSACTION DUE DILIGENCE	COMPLIANCE PROGRAM CONSULTING	COMPLIANCE TECHNOLOGY
ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER (KYC) COMPLIANCE		ANTI-CORRUPTION COMPLIANCE (FCPA, UK BRIBERY ACT)	SUPPLIER DIVERSITY

Contact Kroll for more information:

Americas: + 1 212.833.3208 | EMEA: +44 20 7029.5136 | APAC: +65 6645.4950

kroll.com