Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Focus on Corruption

Sharpening Third-Party Due Diligence

An e-Book publication sponsored by Kroll Advisory Solutions™ An Altegrity Company

Sharpening Third-Party Risk Mitigation

Companies still fall short when it comes to effective third-party due diligence; below, experts offer tips on how to mitigate third-party risks and thwart compliance breaches

By Jaclyn Jaeger

Never has third-party risk management been as high a priority as it is in today's stringent anti-corruption enforcement environment. Yet, many companies still aren't up to snuff when it comes to refining the processes used to mitigate third-party risks.

They are in a "relative state of paralysis," says Kenneth Kurtz, chief executive officer of Steele Compliance & Investigation Services. "What we're experiencing is an environment where companies know they need to do something, but they don't know exactly what to do first." Kurtz says lots of companies have defined policies and a framework in place, but no process to execute those policies.

A high portion of charges of Foreign Corrupt Practices Act violations come from the actions of third parties acting on another company's behalf. That means companies need to have far more knowledge of the entities they transact with. "Know your customer, know your vendor, know who you're doing business with," says Bobby Butler, senior vice president, chief compliance officer, and internal audit director for Universal Weather and Aviation, a global flight planning and flight support services provider.

According to Butler, companies need to develop better tools, processes, and policies for minimizing risks associated with third parties. The first step in that process is to establish a "credible and defensible risk model" for your company, says Kurtz. That risk model should be based on the company's unique risk factors, which should then be weighted and used to calculate a risk score for each third party.

Companies don't have to go it alone on conducting due diligence on third parties. Universal Weather and Aviation, for example, uses a supply chain compliance solution as a starting point on the path to streamline its Level I due diligence process, says Butler. The global platform captures, assesses, and shares baseline due diligence information on organizations and individuals across the supply chain. For example, the system can track the details of an organization and its ownership and scan them against government watch lists.

"Know your business, know your vendor, know who you're doing business with."

—Bobby Butler,
SVP, Chief Compilance Officer, and Internal Audit Director,
Universal Weather and Aviation

The system "takes the financial burden off the company and allows us to reallocate our resources to enhance and increase our Level II and Level III due diligence," says Butler. That involves taking a deeper dive into understanding the risk profile of each third party.

Effective third-party due diligence is not a "one-size-fits-all program," Kurtz says, but rather should be based on each organization's appetite for risk. Employ a risk model that is "realistic for your business, reflective of best practices, and affordable on a long-term basis," he advises.

Testing your risk model and processes before rolling them out is crucial, Kurtz adds. "Some organizations try to roll a program out globally, and they end up committing themselves to a process that is too expensive and too complex for the business," he says.

At Universal Weather and Aviation, each of its roughly 10,000 third parties is scored based on several risk factors, such as geography, or how long the company has been doing business with that third party. One industry-specific risk factor is how many landings occur at a particular airport on an annual basis.

"We take all these factors to develop a risk matrix," says Butler. That allows the company to rank and continuously review each third party from high to low risk. The company refers to outside measures of corruption in the countries it does business in, for example, and adds them to the matrix.

The establishment of that risk model prescribes the next steps for the third-party on-boarding process, which needs to be clearly understood and refined by the business, says Kurtz. Often, however, companies that have implemented a risk model "don't have the resources or defined processes to support the risk model," he says. Due diligence is just one step in an entire third-party on-boarding process.

Companies need to dig deeper into the actual practices of third parties to make sure they align with the policies and procedures on the surface. One of the most daunting challenges when it comes to managing third-party risks, for example, is ensuring that the actions of venders and service providers are "consistent and aligned with the company's code of conduct and core values, so that they're not doing anything that you wouldn't want your own employees doing," says Butler.

For Universal Weather and Aviation, safety is a particularly serious concern. "We send our traffic to some of these third parties, so we have certain service-level agreements and safety standards that we want them to meet," he says.

"What we're experiencing is an environment where companies know they need to do something, but they don't know exactly what to do first."

—Kenn Kurtz,
Chief Executive Officer,
Steele CIS

Trust, but Verify

In addition to anti-corruption training, all third parties have a business sponsor within Universal Weather and Aviation who owns the relationship and is accountable for any actions associated with that relationship, says Butler.

The company also periodically reconfirms the third-party information it has on file and certifies that the information is accurate. Various factors may change in the course of a year, including a third party's risk ownership, revenue stream, business location, and the services they provide. So you need to continually audit and monitor those activities, says Butler.

Including a right-to-audit clause in contracts with third parties is not always the best avenue to take. On the positive side, a right-to-audit clause in contracts with third parties can act as a safeguard to provide more detailed insight into its practices. It gives you a "foot in the door" to understand what the third parties are doing on your behalf," says Butler.

They allow the contracting company to develop a specific audit program with defined scope and objectives to achieve a desired outcome. If your third parties know they can't slip anything passed you, it prevents a whole bunch of compliance lapses from occurring, says Butler.

The disadvantage with incorporating a right-to-audit clause into a third-party contract, however, is that it arguably creates an implied obligation to audit from an enforcement perspective in the event that an issue arises. "If you include a right-to-audit clause and don't audit against them, it makes you look ineffective," says Butler.

Butler and Kurtz agree that if your company does not have the manpower or resources to audit third parties, don't put them in place. Having fewer, clearly defined policies in your program that are actually followed is much better than having more programs that are less defined and not followed at all, says Kurtz.

Universal Weather and Aviation ensures that its processes are reviewed and followed by having in place an operational selection committee. In addition to Butler, other members on the committee include operational vice presidents, as well as the general counsel.

Having an operational selection committee ensures that decisions are being made as a group, rather than on an individual level, says Butler. "It helps minimize service-level deficiencies from occurring," he says, "and it helps minimize compliance breaches that could occur on the ground." ■

Investing in the BRICs

Extra Due Diligence Is Vital

By David A. Holley

The fertile and fast-growing economies of the BRIC (Brazil, Russia, India, and China) countries are calling to international corporations, investment banks, and investors like the Sirens sang to Jason and his shipmates in Argonautica. The haste to take advantage of these burgeoning markets can lead to rushed decisions, shortcuts in diligence, and potentially unmeasured business decisions. Whether a company is entering a new market, contemplating a joint venture with an overseas partner, investing in a foreign business, or acquiring an overseas company, an appropriate level of due diligence on the foreign entity, its agents, business partners, and intermediaries is required to avoid problems associated with current anti-bribery legislation. However, the results of the 2012 Kroll Global Fraud Survey indicate that only half of the respondents believe that their due diligence is sufficient to fully understand whether the acquisition target complies with either the United Kingdom Bribery Act (UKBA) or the United States Foreign Corrupt Practices Act (FCPA). In addition, nearly one-quarter of respondents consider their companies moderately to highly vulnerable to corruption, which is among the leading reasons why companies avoid investing in new regions or countries.

The high level of concern uncovered in the survey may overestimate the true degree of compliance because companies often believe they are doing better in following the law than they actually are. Even if we accept these self-reported estimates, however, there is cause for alarm over the exposure of many corporations to the criminal sanctions and costs imposed by the FCPA and UKBA, particularly in this era of aggressive enforcement by the Department of Justice (DoJ) and Britain's Serious Fraud Office (SFO), respectively. The question then becomes what steps should be taken by a corporation determined to follow the spirit and letter of the law. Managing the anti-bribery risks through heightened due diligence should be a paramount focus when expanding into the BRIC markets and other emerging economies.

There is little guidance in either law as to what constitutes sufficient due diligence. The FCPA makes no mention of the term. The DoJ in "Opinion Procedure Release 08-01" has defined a "reasonable" due diligence file as containing the following: an independent investigative report by a reputable international investigative firm; guidance by a foreign business consultant to help navigate the due diligence in the foreign jurisdiction; reports from the U.S. Commercial Service within the Department of Commerce; the results of various databases and watch lists, DNDB, etc.; meeting notes from discussions with the U.S. Embassy in the foreign jurisdiction; a report by outside counsel on the target; a report on the target company by an independent forensic accounting firm; and an opinion by a second outside counsel who reviewed the sufficiency of the entire due diligence process.

Companies often believe they are doing better in following the law than they actually are.

While the UKBA and SFO provide some direction on due diligence, it also provides a defense for companies that have adequate procedures in place to prevent the type of conduct that would otherwise give rise to prosecution. The Ministry of Justice provides some guidance on "adequate procedures" indicating that due diligence should be conducted on parties performing services for, or on behalf of, a business and that it should be "proportionate and risk-based." With relatively little guidance, it is no wonder that there is so much concern around the adequacy of due diligence undertaken in advance of a business transaction.

Assuming that multi-national corporations are doing some level of due diligence consistent with the guidance offered by American and British regulators, the question as to why the level of anxiety in respondents over the sufficiency of their due diligence remains high. When undertaking due diligence in contemplation of expansion into the BRIC and other emerging markets, consider the following recommendations:

1. The volume of publicly available information varies from country to country and is generally considerably less than what is available, for example, in the United States. In addition, the information is frequently not as well organized or as readily searchable as in many jurisdictions. This highlights

the importance of "feet on the ground" and the ability to undertake discreet source inquiries to fully understand a due diligence subject.

2. The potential for encountering a Politically Exposed Person (PEP) is generally greater in Russia and China than in many other parts of the world. This requires more extensive due diligence on officers, directors, and shareholders than normal to steer clear of violations. An examination of a target's vendors and agents to ensure arm's-length transactions with unrelated parties is also recommended.

3. Media searches may not be as thorough, complete, and reliable as in other jurisdictions, as the local media and press are generally less aggressive and less likely to present an in-depth examination of issues. For instance, in countries like China and Russia, both hotbeds of recent and future M&A activity by Western companies, the simple act of checking available media outlets for information about a potential partner is likely to yield incomplete results at best. This is particularly true in China, where the tradition of an open press is weak and corruption is generally regarded as high.

4. There continues to be an absence of strong anti-corruption laws and enforcement in BRIC countries compared to the United States, the United Kingdom, and other countries. This requires a company to engage in more extensive examinations of acquisition targets' policies, procedures, and employee handbooks relating to corruption, anti-bribery, and gifts and entertainment expenditures.

Understanding the requirements of thorough due diligence is an important step, but problems can also arise when issues turned up in a review are not managed effectively. This point was driven home by the March 2011 settlement involving Ball Corp., a U.S. manufacturer of metal packaging for food, beverages, and household products. In March 2006, Ball acquired an Argentine entity, Formametal S.A. The Securities and Exchange Commission (SEC) found that during the course of Ball's pre-acquisition due diligence, information suggested that "Formametal officials may have previously authorized questionable payments" disguised within the company's books and records. Unfortunately, Formametal executives did not do enough to prevent further improper payments to Argentine customs officials, giving rise to the SEC's case. The SEC noted that Ball Corporation did not promptly terminate the responsible employees when company accountants learned about the improper payments in February 2007. Still, Ball's fine was a relatively small $300,000 because of the company's other remedial efforts, voluntary disclosure of the misconduct, and cooperation in connection with a related investigation.

Participating in the world's fastest-growing economies carries growing risks.

The BRIC economies are enormously attractive investment opportunities. Estimates are that as much as 60 percent of the world's GDP will come from them by 2030. Participating in the world's fastest-growing economies carries growing risks, too. American, British, and multinational corporations need to understand the potential corruption dangers in the BRIC and similar emerging economies and undertake effective due diligence to avoid running afoul of anti-corruption laws. Certainly the DoJ, SEC, and Britain's Serious Fraud Office have recognized the risks and stepped up their scrutiny of activities in these countries as part of the overall trend in rising enforcement of anti-corruption laws globally. ■

ABOUT THE AUTHOR

David A. Holley is a Senior Managing Director and head of Kroll Advisory Solutions' Boston office. With nearly 25 years of investigative experience, David has directed a wide variety of complex assignments and provided litigation support for clients throughout the New England region. His practice areas include environmental matters, contests for corporate control (proxy fights and hostile takeovers), major fraud investigations, internal investigations, due diligence matters, patent infringement and theft of trade secret engagements, crisis management, security and vulnerability assessments, and other sensitive investigations. David also consults with clients on best practices for compliance with the Foreign Corrupt Practices Act, BSA/AML rules and other regulatory regimes.

Not All Third-Party Risks Are Created Equally

By Jaclyn Jaeger

Most companies group third-party risks from agents, resellers, and distributors all under the same umbrella. Yet not all third-party risks are created equally.

Such business partners often have different legal exposures and corruption risk profiles, effecting the level of due diligence that a company must conduct on each.

Taking a risk-based approach to third-party due diligence helps senior management allocate resources more effectively. "A full due-diligence profile is not always necessary," says David Simon, a partner at law firm Foley & Lardner. "You have to look at what the relationship is pretty carefully to judge the level of compliance measures that are required."

> "If [distributors] are off paying bribes, and you know about it and don't do anything to stop it, you're almost certainly going to be held responsible for their actions."
>
> —David Simon, Partner, Foley & Lardner

Distributors often pose greater risks, for example, than resellers or agents and tend to require a higher level of scrutiny when it comes to compliance with the Foreign Corrupt Practices Act, because companies have less control over them. Whereas resellers and agents sell products and services on a company's behalf, distributors are independent parties who buy, and assume title of a company's products to resell into other markets, potentially including high-risk foreign markets.

Companies have far less leverage to demand audit rights and training on anti-corruption measures with distributors, since they often supply several manufacturers' products at once, including competitors' products. "You can't approach those distributors and realistically expect them to give you audit rights," says Simon. As a result, companies often have a difficult time mitigating the corruption risks posed by distributors, especially those in high-risk foreign markets.

Despite these compliance challenges, the Department of Justice and the Securities and Exchange Commission have offered no shortage of cases in which companies have been found liable where their distributors have violated the FCPA. "If [distributors] are off paying bribes, and you know about it and don't do anything to stop it, you're almost certainly going to be held responsible for their actions," says Simon.

In one example, software giant Oracle in August agreed to pay a $2 million penalty to the SEC for charges of violating the FCPA by failing to devise and maintain a system of effective internal controls that would have prevented its India subsidiary from secretly setting aside money off the company's books that enabled Oracle India's distributors to make unauthorized payments to phony vendors in India.

According to the complaint, Oracle India sold software licenses and services from 2005 to 2007 to India's government through local distributors, and then directed the distributors to "park" the excess funds—approximately $2.2 million—from the sales outside Oracle India's books and records. Such practices, the SEC complaint stated, "created the potential that [the payments] could be used for bribery or embezzlement."

In another case, medical-equipment manufacturer Smith & Nephew in February entered into a deferred prosecution agreement and agreed to pay a total of $22 million in fines and penalties to the Justice Department and the SEC in connection with bribes paid by Smith & Nephew's affiliates, subsidiaries, employees, and agents to publicly employed healthcare providers in Greece from 1998 to 2008 to persuade them to purchase medical devices manufactured by the company.

Tom Fox, an independent FCPA compliance consultant and lawyer, says one warning the Smith & Nephew case provides is that companies must carefully consider the commission payments they pay to distributors. In the eyes of enforcement authorities, any commission paid to a foreign business representative is the amount that could be used to pay bribes. "It's one thing to get 5 to 10 percent of a sale and another to get 30 percent," he says.

In this particular case, Smith & Nephew sold its products at full list price to a Greek distributor then paid the amount of the distributor discount—between 25 and 40 percent of the sales made by the distributor—to an off-shore shell company controlled by the distributor.

"As a company, you have to be able to justify the higher rate that you pay to the distributor," says Fox. Exactly what the Justice Department considers an appropriate rate is not quite clear, due to a lack of case law, "but that is something that companies need to pay very close attention to," he says.

Risk Assessment

Many companies maintain vendor master lists and third-party databases that span hundreds—if not tens of thousands—of distributors and other third parties, making it unreasonable to run background checks on every one of them. The practical way to minimize FCPA risk associated with a global distributor network without devoting an unreasonable amount of time and money toward compliance efforts is to conduct a risk analysis to determine which third parties pose the highest risks, says Simon.

On the low-risk end, for example, are distributors that have little affiliation with the company. Many distributors are more like customers than agents, who merely purchase a product and resell it to others. "If they're really just a reseller or a customer, and all they're doing is buying your product and selling it along with other products, I think you can get away with a lot less, and I think it's appropriate to do a lot less," says Simon.

On the high-risk end, however, are distributors that are very closely tied to the company, who effectively represent the company in the market. "The more that they look like you in that market, the more likely it is that you're going to be responsible if they pay a bribe," says Simon.

Once a company distinguishes what distributors pose a low risk of FCPA liability versus those that pose a high risk, "the question then becomes, what steps do you need to take, absent a red flag, to ensure that they're not engaging in conduct that would be prohibited by the FCPA?" says Simon.

At a base level, companies may want to include right-to-audit and termination clauses in contracts with third parties and FCPA training and certification, says Simon. Other typical third-party due diligence practices include running risk screenings of sanctions watch-list databases, checking public records such as court filings, and conducting Internet searches. In high-risk country operations, additional due diligence procedures may involve in-country searches that include site visits and reference checks.

How much due diligence is enough depends on each company's own risk profile. Comverse Technologies, for example, has a "very stern anti-corruption policy, and we make all our third-party go-to-market channels—whether it be agents, resellers, or distributors—acknowledge that they're aware of it and what's expected of them," says David Frishkorn, chief compliance officer at the $1.6 billion technology company.

Traditionally, when it comes to conducting third-party due diligence for FCPA compliance, cost has been a big concern, notes Frishkorn. Today, that's not so much the case anymore.

Not only is there more competition among service providers who offer due diligence services, Frishkorn says, but also in this digital age companies literally have at their fingertips more information on their third parties than ever before—both of which significantly drive down the time and cost of conducting due diligence.

Despite some minor legal nuances that may exist regarding who owns the title of a product and who legally represents the customer, "at the end of the day, it's always my product or service that's going to end up in the hands of the consumer," says Frishkorn, "I bear some direct legal risks or, certainly, reputational risk." ■

FCPA PROBE RESOLUTION

Below is an excerpt from the Justice Department's release regarding Smith & Nephew:

According to the criminal information filed in U.S. District Court in the District of Columbia in connection with the agreement, Smith & Nephew, through certain executives, employees and affiliates, agreed to sell products at full list price to a Greek distributor based in Athens, and then pay the amount of the distributor discount to an off-shore shell company controlled by the distributor. These off-the-books funds were then used by the distributor to pay cash incentives and other things of value to publicly-employed Greek health care providers to induce the purchase of Smith & Nephew products. In total, from 1998 to 2008, Smith & Nephew, its affiliates and employees authorized the payment of approximately $9.4 million to the distributor's shell companies, some or all of which was passed on to physicians to corruptly induce them to purchase medical devices manufactured by Smith & Nephew.

The agreement recognizes Smith & Nephew's cooperation with the department's investigation, thorough self-investigation of the underlying conduct, and the remedial efforts and compliance improvements undertaken by the company. As part of the agreement, Smith & Nephew will pay a $16.8 million penalty and is required to implement rigorous internal controls, cooperate fully with the department and retain a compliance monitor for 18 months.

In a related matter, Smith & Nephew reached a settlement today with the U.S. Securities and Exchange Commission, under which Smith & Nephew agreed to pay $5.4 million in disgorgement of profits, including pre-judgment interest.

This case is being prosecuted by Trial Attorney Kathleen M Hamann of the Criminal Division's Fraud Section with assistance from the FBI Washington Field Office's dedicated FCPA squad.

The Justice Department acknowledges and expresses its appreciation for the assistance provided by the authorities of the 8th Ordinary Interrogation Department of the Athens Court of First Instance and the Athens Economic Crime Squad in Greece, as well as the significant coordination with and assistance by the Securities and Exchange Commission's Division of Enforcement.

Source: Justice Department.

The Struggle to Tame Third-Party Corruption Risk

By Jaclyn Jaeger

Corporate compliance departments are increasingly uneasy about their exposure to bribery risks, and many say they are still not up to snuff when it comes to policing third parties and eliminating facilitation payments.

According to a recent study from Kroll Advisory Solutions, 69 percent of 139 compliance executives surveyed say their companies have either high or moderate exposure to bribery risk. And in the pharmaceutical industry, all of the respondents say risks are high or moderate.

The biggest concern comes from corruption risks related to third parties, such as resellers, distributors, agents, or joint-venture partners. "In general, companies are still incredibly uncomfortable about the process of managing third parties," says Bill Pollard, a partner in Deloitte's Foreign Corrupt Practices Act consulting practice.

The Kroll study comes at a time when several oil giants, including Chevron and ExxonMobil, have launched internal investigations over allegations of bribery payments made on behalf of the companies to customs officials in Kazakhstan.

The probes illustrate the difficult time companies that operate in emerging markets are having of mitigating third-party corruption risk. One of the greatest challenges for companies is simply identifying all of their third parties, never mind the due-diligence that then needs to be performed, says Pollard.

Once they do, they should conduct risk assessments to identify those that require more attention than others. Some companies end up spending more money than they need to by conducting the same level of due diligence on every third-party, says Alexandra Wrage, president of TRACE International, a non-profit association that provides anti-bribery compliance solutions. "That just isn't sustainable," she says.

At the other end of the spectrum are companies that are not doing anything at all to rein in third-party corruption risks and are paralyzed because they don't know how to get started. "Both of those extremes are bad for business and bad for compliance," Wrage adds.

According to the Kroll study, 71 percent of respondents say their companies require third parties to list any affiliations they have with foreign officials, 65 percent verify that third parties adhere to the company's code of ethics, and 73 percent confirm that each third party is free from sanctions pertaining to compliance with anti-bribery regulation. Twelve percent said they conduct no due diligence on third parties at all.

Part of the problem for many companies is a lack of a centralized system to send, collect, and analyze third-party questionnaires, the Kroll study found. Of the 71 percent of respondents from companies that require third parties to complete questionnaires, 60 percent say they use a manual, paper-based process.

That's far too high say FCPA experts. "We're never going to get rid of the element of judgment, nor should we try, but what technology can do is key things up and take away a lot of the repetitive work and help with storage, sourcing, and prioritizing," says Wrage. "Those are all very important."

Some industries are farther along in the process than others. While pharmaceutical companies are the most concerned about bribery risk, they are also the most vigilant about managing third-party risk. For example, 100 percent of drug company respondents say they conduct screening to confirm each third party is free from sanctions pertaining to compliance with anti-bribery regulations, compared to 65 percent in all other sectors. They were also unanimous in having policies that prohibit facilitating payments, compared to 87 percent of all respondents who say they prohibit such payments.

David Holley, a senior managing director at Kroll who co-authored the survey, reasons that pharmaceutical companies rely very heavily on third parties—from drug testing to packaging to market approval—that it's "really prepared them very well for what needs to be done in the FCPA context."

The Kroll study also revealed that companies tend to have more control over their employees than their third parties; nearly all respondents (99 percent) said they had anti-bribery provisions for employees in their companies' codes of conduct, but only 73 percent have the same in place for third parties. While that number is good, "it should be higher," says Holley.

M&A Transactions

The study also found that more companies are conducting rigorous due diligence on mergers and acquisitions to identify and mitigate corruption risk. In fact, that work is leading to changes in merger terms or even scuttling deals altogether when FCPA red flags appear, according to Deloitte's Pollard. As companies continue to invest in emerging markets, "the request to do anti-corruption due diligence as part of an overall risk assessment is significantly on the rise," he says.

Findings from the Kroll study reveal a similar trend. Eighty-one percent said they require the other party to complete due diligence questionnaires to vet their compliance levels with anti-bribery regulation.

Additionally, 78 percent reviewed existing contracts and third-party relationships of M&A targets to minimize noncompliance with regulations; 65 percent reviewed their target companies' third parties for potential corruption; and 48 percent screen the targets of third-party acquisitions. Nineteen percent of all respondents said they abandoned or re-negotiated a merger or acquisition as a result of failed anti-bribery compliance.

Facilitation Payments

The survey also identifies some surprising views on facilitation payments. While 60 percent of respondents said they do not permit facilitating payments for any reason, 36 percent said that they do under certain circumstances. That's "quite surprising," says Holley. "Those that I talk to have no tolerance for facilitation payments at all."

"The trend is definitely moving toward no facilitation payments," says Pollard. More and more companies are putting such prohibitions into their policy or program in some way, he says. In the Kroll study, just 19 percent said they do not have a written policy to address facilitation payments.

Companies that have been silent on the issue in the past are either "severely restricting" or becoming more explicit about the rare instances when a facilitation payment would be allowed, such as the threat of the loss of life, says Pollard.

Most all respondents of the Kroll study believe their bribery risks have increased or held steady over the last few years and expect that to continue. Because of the increased enforcement in the United States and overseas and the overall trend toward more cooperation among enforcement agencies, "things are going to get worse before they get better," says Wrage.

The good news is that compliance departments are investing more in their anti-bribery efforts. Fifty-three percent of respondents said their compliance budgets had increased, and 49 percent said their compliance departments had increased hiring.

Most respondents also expressed confidence in their anti-bribery compliance programs, especially as it applies to effective policies and procedures (56 percent) and anti-bribery training (31 percent).

The top initiatives companies are implementing to minimize bribery risk include: employee training (60 percent) and establishing executive-level commitment to anti-bribery measures (23 percent).

Education and training are important, but foremost is adopting a policy from the top down throughout the entire organization, says Holley. One example is having senior executives pay visits to the company's offices overseas to personally discuss the importance of compliance. "As small and remote as a part of a business might be," he says, "it could really affect an entity's compliance track record." ■

RISK EXPOSURE

The following chart from Kroll Advisory Solutions explores specific industries' exposure to bribery risk.

While perceived exposure to risk varies from industry to industry, the majority of compliance executives participating in the survey expressed vulnerability to bribery risk. Sixty-nine percent of all respondents said their companies were either moderately or highly exposed to bribery risk; this number jumps to 100 percent in the pharmaceutical industry and drops to 46 percent in the financial services industry.

Perceived Exposure to Risk Related to Compliance With Anti-Bribery Laws

By Industry					
	All Respondents	Financial	Energy	IT/Telecom	Pharma
Our company is highly exposed to risk related to anti-bribery regulations	24%	8%	33%	25%	54%
Our company is moderately exposed to risk related to anti-bribery regulations	45%	38%	40%	50%	46%
Our company has only limited exposure to risk related to anti-bribery regulations	19%	31%	20%	11%	--
Our company has no significant exposure at all	12%	21%	7%	14%	--

Source: Kroll Advisory Solutions.

Justice Department Ends DPA Early, Citing Robust Compliance

By Jaclyn Jaeger

In a rare case, the Department of Justice agreed last month to end a deferred prosecution agreement related to alleged violations of the Foreign Corrupt Practices Act one year early.

The case also marks the first time the Justice Department has expressed—at least publicly—its willingness to relax enforcement of successor liability in situations where the acquiring company has in place a robust compliance program and expresses a commitment to prevent further violations. Successor liability in the FCPA context occurs when one company inherits the FCPA violations of another company through an acquisition.

> In light of the foregoing circumstances, the government has determined that the continued deferred prosecution of Pride is no longer warranted.
>
> —Department of Justice

In November 2010, offshore drilling company Pride International entered into a three-year DPA with the Justice Department to settle allegations of illegal bribes paid to government officials in Venezuela, India, Mexico, and other countries in order to extend drilling contracts and obtain other improper benefits from 2001 to 2006. Pride was acquired by Ensco, a British provider of offshore drilling services, in May 2011, which then took on the requirements of the DPA.

Under the DPA, Pride paid a $32.6 million criminal fine and agreed to adhere to the following compliance procedures:

- Institute and maintain a compliance and ethics program that is designed to prevent and detect violations of the FCPA;
- Maintain internal controls, policies, and procedures to ensure that books, records, and accounts are fairly and accurately made and kept; and
- Reduce its reliance on third-party business partners and subject them to appropriate due-diligence requirements pertaining to the retention and oversight of agents and business partners.

"Pride has fully met its obligation under the DPA of cooperating with the United States," the Justice Department stated in its motion to free Pride of its agreed commitments early. "In light of the foregoing circumstances, the government has determined that the continued deferred prosecution of Pride is no longer warranted."

"Pride hit all the marks of effective compliance and good governance," says Jan Handzlik, a partner with law firm Venable. For the Justice Department to recognize these efforts is a "hopeful sign and a further indication of the benefits of disclosure and cooperation," he says.

In a related motion, the Justice Department also agreed to end the unsupervised probation period imposed on Pride Forasol, Pride's French drilling subsidiary, citing similar compliance improvements. U.S. District Court Judge Lynn Hughes granted the dismissals for both motions on Nov. 2.

"The sentence imposed reflected the seriousness of the offense and has promoted respect for the law and 'adequate deterrence' against international corruption," the motion to dismiss stated. "The government, therefore, has determined that no further purpose of the United States in the enforcement of the federal criminal laws would be served by continuing the term of probation imposed on Pride Forasol."

In addition to Pride's own compliance undertakings, Ensco's commitment to honor the DPA following its acquisition of Pride also appears to have played a role in the early dismissal of the DPA.

With its acquisition of Pride, Ensco additionally represented to the Justice Department a high-level of anti-corruption oversight, with its general counsel, chief compliance officer, and director of internal audit all directly reporting to the chair of the audit committee.

The Pride case is unusual "in the sense that Pride had already entered into the DPA at the time it was acquired by Ensco, as opposed to Ensco finding evidence of FCPA violations during the pre- or post-acquisition due diligence on Pride," says Valarie Hays, a partner in the corporate compliance practice and the litigation practice at law firm Schiff Hardin.

"Presumably, the Justice Department dismissed the DPA early because Ensco had a strong and effective compliance program in place," Hays adds. "A company can minimize its chances of successor liability by doing exactly what Ensco did: putting an effective compliance program in place and immediately incorporating newly acquired companies into that program."

The Justice Department declined to comment beyond the filings it has made in the case. Ensco also declined to comment.

Other Examples

Paul Pelletier, a member in the litigation section of law firm Mintz Levin, says that it is not unprecedented that the government would permit early termination from the terms of a DPA. “Upon objective and independent proof that a deferred company’s anti-corruption compliance program is now working and effective, government prosecutors have often shown a willingness to terminate potentially onerous supervision conditions,” he says.

Mike Koehler, a law professor at Southern Illinois University and better known for his blog, “the FCPA professor,” points to another case, where the Justice Department filed a motion to dismiss criminal charges in April against pipeline construction company Willbros, stemming from legacy issues in Nigeria and South America in 2005 and prior years, resulting in the DPA.

During a recent earnings conference call, Willbros stated that the motion to dismiss followed the company’s completion of the requirements of the DPA and the expiration in March of the terms of its compliance monitorship. On April 2, a U.S. District Court judge in Texas signed an order of dismissal of all charges.

“We are pleased to have successfully completed the requirements of the DPA and the monitorship,” Willbros CEO Randy Harl said during a recent earnings conference call. “Willbros is committed to compliance with the law, and we have instituted values and processes that we believe will prevent any future FCPA-related incidents.”

Only in the last few months has the Justice Department been especially vocal about doling out credit for having robust internal controls. For example, the Pride International case together with the Morgan Stanley case, “while two very different situations,” both send the same important message to companies that “the Justice Department does take into account compliance procedures,” says Tom Gorman, a partner with Dorsey & Whitney.

In the Morgan Stanley case, the Justice Department opted not to bring an enforcement action over violations by one individual of the FCPA, similarly citing the company’s compliance program as the reason for declining to prosecute.

With each case study, companies should be comforted to know that cooperation credit with the government isn’t hopeless. “There’s no reason why the Department of Justice shouldn’t have the flexibility and discretion to dismiss a case early,” Nardello says, “if they believe the goal and the conditions of a deferred prosecution agreement have been met.” ■

MOTION TO DISMISS

Below is excerpted and summarized from the Justice Department’s Unopposed Motion to Dismiss Criminal Information:

On November 4, 2010, the United States filed a criminal information charging Pride with conspiracy to violate the anti-bribery provisions of the Foreign Corrupt Practices Act. On the same date, the United States also filed a three-year deferred prosecution agreement it entered with Pride. While the DPA was for a three-year period, the DPA also provides that “in the event the Department finds . . . that there exists a change in circumstances sufficient to eliminate the need for the corporate compliance reporting obligation” in the DPA, the DPA may be terminated early.

As part of the DPA, Pride agreed to acknowledge responsibility for the actions of its employees and agents. Pride also agreed to pay a $32,625,000 monetary penalty and to continue to cooperate with the United States and adhere to certain compliance undertakings. Pride has fully met its obligation under the DPA of cooperating with the United States.

... On or about May 31, 2011, Ensco plc acquired Pride in a merger and assumed the obligations of Pride under the DPA. Ensco has represented that after the merger, (a) Pride’s business units have become subject to Ensco’s compliance and ethics program, which is designed to prevent and detect violations of the FCPA; (b) that Ensco maintains internal controls, policies and procedures to ensure that books, records, and accounts are fairly and accurately made and kept; and (c) that Ensco conducts appropriate due diligence pertaining to the retention and oversight of agents and business partners. Ensco has further represented that its general counsel, its chief compliance officers, and its director of internal audit are responsible for the implementation and oversight of compliance with policies, procedures and internal controls regarding the FCPA and other applicable anti-corruption laws across the entire Ensco organization, and that these corporate officers report directly to the chair of the audit committee of the board of directors.

In light of the foregoing circumstances, the government has determined that the continued deferred prosecution of Pride is no longer warranted. Accordingly, the United States moves to dismiss the criminal information filed against Pride at this time.

In a related motion, the United States is moving to terminate the term of unsupervised probation imposed on Pride Forasol.

Source: Justice Department.

Third-Party Compliance

Part of a Comprehensive Compliance Policy

By David A. Holley and Thack Skidmore

Corporations have made real strides over the past decade in their efforts to assure compliance with anti-bribery regulations such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act. They are beefing up their anti-bribery compliance budgets, hiring additional compliance personnel, and centralizing compliance decision making. Dig beneath the surface, though, and a different story emerges. While many companies have compliance policies in place, implementation standards vary widely. Such a discrepancy in implementation standards is most pervasive in the implementation of compliance procedures for third-party business partners, where the greatest threat of bribery corruption resides.

While it is important for companies to act now to ensure they are performing due diligence on third parties, it also is important that they make those anti-bribery compliance programs part of a broad and holistic anti-bribery policy. Too often, companies create their policies in isolation to address specific areas of risk, such as facilitation payments or supervising managers in foreign locations. A better approach is to reassess the company's anti-bribery program in total, and then set about creating a comprehensive policy that assures compliance not just in specific areas of focus but across the enterprise, covering both internal (employee) and external (third-party) threats. The objective is not merely to meet the letter of the law in narrowly defined areas, but to embrace the spirit of the law on a broad front, and in doing so create a better business organization.

> *One of the things implicit in the FCPA and almost explicit in the U.K. Bribery Act is that you must not only do the right thing, you must be seen to have done the right thing.*

A comprehensive policy, well implemented and well documented, will prove important in the event a bribery allegation is investigated by regulators or prosecutors. Being able to show that you performed robust due diligence and show what you found, including no red flags, does not mean your company will not face repercussions from regulators or prosecutors. However, it will be considered a mitigating factor in assessing punishment in the United States and Canada, according to an anti-corruption expert, and could be a complete defense in the United Kingdom. Simply telling regulators what you did isn't enough, she stresses. They will want to see that what you did was part of your written code and was acted upon in the context of a comprehensive and enforced policy.

"One of the things implicit in the FCPA and almost explicit in the U.K. Bribery Act is that you must not only do the right thing, you must be seen to have done the right thing," she adds. "The more carefully documented you are, the easier it is to defend against a claim. You want to have your processes and procedures appropriately recorded. It's much more difficult and expensive to do it after the fact."

Many resources are available to help companies craft anti-bribery compliance policies. Beyond the very specific advice they can offer, experience has shown that the most effective policies tend to share these characteristics:

» **Broad authority, stressing both the letter and the spirit of the law.** A strong anti-bribery program must identify the specific types of behaviors and activities that are disallowed, simply to make them as clear as possible to employees, business partners, and third parties. But it also should outline the principles of compliance, explaining why bribery is wrong, what anti-bribery laws seek to accomplish, and how compliance with those laws can help the company become a more efficient and accomplished competitor. Put another way, a strong anti-bribery program must be more than a mindless tick-the-box exercise, but it must be that, too. Yes, companies must be able to document that every employee has been informed of the practical provisions of the FCPA, the U.K. Bribery Act, and other anti-bribery laws pertinent to their work. The more carefully processes and procedures have been documented, the easier and cheaper it becomes to defend against a claim. But box-ticking alone will not ensure that employees understand and have bought into the need for, and advantages of, complying with anti-bribery laws.

» **Full and visible backing from the executive suite.** It's become rote to say that tone at the top matters, but it remains no less true. Senior management must clearly and publicly endorse the message that bribery will not be tolerated, and that

Kroll Advisory Solutions
An Altegrity Company

it is, in fact, antithetical to the interests of the business.

» **Identifiable leadership.** U.S. Federal Sentencing Guidelines for Corporations encourage companies to have employees specifically vested with compliance responsibilities, and it is considered best practice for those employees to have dotted-line reporting responsibility to the audit committee of the board of directors. Authorities also expect that boards and audit committees will investigate promptly where illicit behavior is suspected.

» **Training—formal and ongoing.** An anti-bribery policy that is allowed to reside exclusively on bookshelves or in the electronic recesses of the corporate intranet quickly becomes stale and ineffective. Training programs, for employees and third parties, must be proactive, ongoing, engaging, and substantive. Most companies find it useful to employ multiple training techniques: in-person seminars and role-playing exercises, online classes, Webcasts, even reminder bulletins distributed via e-mail or internal publications. One compliance officer who responded to the Kroll survey says his company is creating guidelines for day-to-day decisions in the form of a "cheat sheet" employees can use in their daily work processes. In foreign locales, training should be conducted in the local language, and policy should be translated into the local language. That was made clear in a recent SEC enforcement action with a Texas-based company that settled charges of bribing Mexican officials. In the settlement, the SEC said the company did not have an effective FCPA compliance policy or training program because it was presented to a subsidiary's employees only in English and that those employees were unlikely to be able to understand them in that language. As Jeffrey Cramer, Managing Director of Kroll's Chicago office, notes, "You can't expect people not to break

Doing Business Without Bribery—Where Bribery Is the Norm

For companies operating in parts of the world where bribery is a routine part of the business landscape, combating it isn't just a moral or legal challenge but a cultural one, too.

"There are 'expectations' embedded in the business practices of countries we do business with," observes a compliance officer responding to Kroll's recent FCPA Benchmarking Survey. "Getting them to understand how we operate is difficult."

One survey respondent recalls receiving "requests for proposals" from hospitals in Syria and Iraq that insisted his company would have to send 15 doctors to Las Vegas for "training" as part of any deal.

The remedy for such demands, compliance experts say, is often as simple—and as hard—as taking a firm stand on the issue, and letting it be known that your company will not engage in the practice of paying for business.

"In many places, local authorities or business people are willing to take a bribe—if you're willing to offer," says Tommy Helsby, Chairman Eurasia for Kroll Advisory Solutions. "If you go in with the presumption they are going to ask, suggesting that you are willing to offer, they will try to take advantage of that. But the experience of companies that have gone in with a different attitude has been that people in those countries and industries really don't take bribery for granted, and are willing to be pushed back against."

There are, to be sure, exceptions. When negotiating oil concessions in Africa, for example, it's normal to issue a signing bonus to the person granting the concession. And it's not unheard of for that money to go into the oil minister's pocket. One way for a company to avoid that—or at least avoid liability—is to write the check payable to that country's oil ministry rather than the oil minister, and then invite the press to document the presentation of the check. If the oil minister steals the money from his own ministry afterward, that cannot be blamed on the company. "You've moved the problem into his court rather than yours," Helsby says. "But as soon as you start going along with him and calling the payment 'the oil minister's signing bonus' and sending it to a Cayman Island bank account, you're compromised."

In short, companies develop reputations, just like people. Those that develop a reputation for succumbing to extortion invite more of it. Those that develop a reputation for playing by the book tend to be solicited less. Does it always work? No. In those cases, companies committed to ethical business simply must walk away from the deal at hand.

the law if they don't know what the law is."

"The fact that we focus on (training) employees is our strength," confirms a respondent to the Kroll survey. "You can have policies, but unless the employees own the policy, it's not effective. Empower employees—compliance is everybody's job. You need to be constantly marketing your ethics to employees."

» **Flexibility, along with sensitivity to the organization's needs and circumstances.** The best anti-bribery compliance programs are tailored to the organizations that create them, and take into account, among other things, whether the compliance function is centralized or decentralized. They're also flexible, especially in the area of third-party due diligence, where efforts must take into consideration where the third party is located, what industry it operates in, its size, and its criticality to the company's supply chain. "As our company expands globally, we cannot just cut and paste policies without any regard for local practices," says a respondent to the Kroll survey.

» **A specific focus on third-party risk.** Because so much anti-bribery risk relates to third parties, best-practice compliance policies should include a section devoted specifically to them, spelling out exactly what risks are being targeted, how compliance personnel will assess those risks, and how they will perform due diligence. This section also should explain how third parties and their employees will be trained to comply with the policy, how third parties and their employees will have access to reporting hotlines, and how compliance personnel will monitor and report on the policy's results.

» **A proactive mission.** Best-practice organizations don't just wait for evidence of wrongdoing to appear, but continually look for its telltale signs. Some use data analytic software to analyze third-party transactions for unusual activity that doesn't conform to previous patterns or other known information.

Proactive organizations also operate with elastic boundaries, making themselves more valuable to the enterprise than those operating with tight restrictions. "The best compliance officers don't just tell business leaders what they can't do to win mining business in the Congo or get an oil concession in West Africa," explains a compliance expert. "They also tell them what they can do." (See sidebar: *Doing Business Without Bribery Where Bribery Is the Norm*) "If you're doing due diligence," he adds, "don't ignore the pipe going out the back door and into the river just because your job is FCPA compliance."

This expert also encourages compliance personnel to share with their colleagues information that could help them work more efficiently or effectively with a third-party vendor—even if it has nothing to do with bribery. "Compliance officers need to give practical support to the business," he insists. "The costs of compliance are high, so it makes sense to embrace a broader agenda that allows you to capture the full value of your investment."

Audit and testing. Gauging the effectiveness of a third-party compliance program requires testing. Best-practice companies conduct periodic internal audits to look for red flags or suspicious payments, receive written reports of third parties' actual activities, and exercise their audit rights with third parties. Some also require that payments over a certain threshold be signed not only by a manager in the field but by a second person in another location. While not foolproof, this provides evidence to authorities that the company was making an effort to prevent illicit bribes. One compliance officer responding to the Kroll survey says his company requires its compliance department to pre-approve every payment to a government entity.

By taking a proactive approach to anti-bribery compliance—by doing things like actively and repeatedly training employees, conducting periodic internal audits, and employing data analytic software to analyze third-party business transactions—best-practice companies are making it harder for regulators or prosecutors to argue that those companies ever condoned bribery. "All these practices are far better than just giving employees a piece of paper when they start work that tells them bribes are unacceptable," Cramer asserts. "That played 10 or 15 years ago. It doesn't work anymore." ■

ABOUT THE AUTHORS

David A. Holley is a Senior Managing Director and the head of Kroll Advisory Solutions' Boston office. He can be reached at DHolley@kroll.com

Thack Skidmore is a Director of third party screening and is based out of Kroll Advisory Solutions' Los Angeles office. He can be reached at TSkidmore@kroll.com

COMPLIANCE WEEK

Compliance Week, published by Haymarket Media, Inc., 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.

Founded in 2002, Compliance Week has quickly become one of the most important go-to resources for public companies; Compliance Week now reaches more than 26,000 financial, legal, audit, risk, and compliance executives.

Kroll Advisory Solutions™

An Altegrity Company

Kroll Advisory Solutions, the global leader in risk mitigation and response, delivers a wide range of solutions that span investigations, due diligence, compliance, cyber security and physical security. Clients partner with Kroll Advisory Solutions for the highest-value intelligence and insight to drive the most confident decisions about protecting their companies, assets and people.

Kroll Advisory Solutions is recognized for its expertise, with 40 years of experience meeting the demands of dynamic businesses and their environments around the world. Headquartered in New York with offices in 29 cities across 17 countries, Kroll Advisory Solutions has a multidisciplinary team of 700 employees.

Kroll Advisory Solutions is an Altegrity company. Learn more at www.krolladvisory.com.

Investigations and Third-Party Due Diligence

- » World-Class Investigations, Consulting, and Forensic Accounting Expertise
- » Programmatic Third-Party Due Diligence Platform
- » Global Presence—Unrivaled Experience

Kroll Advisory Solutions℠

An Altegrity Company

600 Third Avenue | New York, NY 10016 | 212.593.1000 | www.krolladvisory.com

Regional offices include: Boston, Chicago, Dubai, Hong Kong, London, Los Angeles, Mexico City, Miami, Moscow, New York, Philadelphia, San Francisco, Tokyo