Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Combatting Corruption

An e-Book publication sponsored by acl transforming audit and risk

COMPLIANCE WEEK

Compliance Week, published by Wilmington 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.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

ACL delivers technology solutions that are transforming audit, compliance, and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allow organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Visit us online at www.acl.com

Inside this e-Book:

Sweating the Small Stuff on Facilitation Payments

Big concern: Refusing to make small bribes can often result in frustrating delays in moving goods, and it can impede operations

by Jaclyn Jaeger

Faced with a global crackdown on corruption, more companies are putting zero-tolerance policies in place for bribery.

Eliminating small bribes and facilitation payments throughout the organization, however, can be a difficult undertaking.

Part of the problem is that small payments are sometimes requested in urgent situations, in which employees are forced to make crucial judgments on the fly, and sometimes even in threatening situations. And refusing to pay even a small bribe can result in delays in moving goods through customs or holding up entire shipments at ports and canals, bringing a company's operations to a grinding halt.

On the demand side of the equation, requests for small bribes are often woven into the fabric of many cultures. Local employees in high-risk jurisdictions who may be used to paying bribes in every aspect of their personal life may not understand why it's unacceptable from a corporate policy perspective. "It's very difficult in some cultures to try to force that distinction," says Julian Glass, managing director for the forensic and litigation consulting practice of FTI Consulting.

Distinguishing between permissible facilitation payments and illegal bribes can also prove maddeningly difficult to navigate, especially when contending with a complex web of global anti-corruption laws. "There is a very thin line between facilitation payments and bribes," Julia Bailey, a managing director and compliance practice leader with BDO Consulting. "A lot of people get tripped up on that."

Companies that adopt a zero-tolerance policy on paying small bribes hope that they can eliminate the expectation from government officials in countries where they do business. "They are starting to find that their reputation for not paying bribes means they are no longer asked; whereas those that pay small bribes can be subject to an ever-increasing spiral of demands," notes a recent report from Transparency International that provides guidance to companies on countering small bribes.

Facilitation payments—also called "grease payments"—are small sums given to foreign officials to expedite normal business transactions, such as clearing goods through customs. They differ from bribes, which are typically meant to entice foreign officials to commit acts they might otherwise not do, such as awarding a contract. "In many cultures, if not most, small grease payments are not considered bribes at all, but more like what tipping in a restaurant would be for us," Bailey says.

Where to draw the line between bribes and facilitation payments can be tricky. For example, if you regularly pay a customs official to get goods over the border, and expect preferred treatment because of the payment, "it's no longer a facilitation payment," Bailey says. "It's a bribe."

No-Bribe Policies

Not until passage of the U.K. Bribery Act in 2011, which imposed a blanket ban on bribes and facilitation payments paid to government and non-government officials, did many multinational companies really begin to assess their policies on facilitation payments. "More companies are adopting a no-bribe policy for their global operations that include no facilitation payments," says Joseph Spinelli, managing director in the global investigations and compliance practice at Navigant Consulting.

The only exception some companies are willing to make is for the physical safety of employees. According to global bank HSBC's anti-bribery policy, for example, "all forms of bribery, including facilitation payments—except in order to protect against loss of life, limb, or liberty—are prohibited, whether they take place directly or indirectly through another party."

> "There is a very thin line between facilitation payments and bribes. A lot of people get tripped up on that."
>
> Julia Bailey, Managing Director & Compliance Practice Leader, BDO Consulting

Aluminum producer Alcoa has in place a similar anti-corruption policy. Adopted in May 2012, it states: "Should a person covered by this policy encounter a situation that presents an imminent and serious safety risk to personnel or company facilities if a payment demand is not met, such a payment would not be a prohibited bribe under this policy."

'Small Bribe' Defined

Other companies are becoming increasingly explicit about what constitutes a small bribe. Cisco, for examples, spells out in its anti-bribery policy a long list of items that may constitute a bribe.

"A bribe is not just cash in an envelope passed under a table," Cisco's policy states. "International laws and Cisco policy define a bribe as 'anything of value,' such as gift cards, home repairs, tickets to a theater or sporting event, guest passes to a private club, a no-bid contract, a summer job for a teenage family member, free limo or courtesy car service rides, and more."

Rockwell Automation offers its employees a list of ac-

ceptable and unacceptable gifts. "Common examples of acceptable gifts include: flowers, food baskets, pens, or notebooks," the policy states. "Examples of unacceptable gifts in a business context may include jewelry, a cruise, limousine ride, a spa treatment, or even securing admission for a customer's child at a school or university."


Spinelli

What constitutes a small bribe is also relative to the jurisdiction where the company operates. In Western culture, for example, a $5 or $10 bribe might be considered insignificant, while in other parts of the world such an amount could equal a person's entire weekly wage, Glass says.

Another common caution about paying small, seemingly insignificant sums is that they add up. Many small bribes, taken together, can quickly amount to large-scale bribery. "You could pay a small bribe once, but what happens if you pay it a multitude of times? Then the small bribes become one large amount," Spinelli says. "That's where companies constantly get themselves in trouble."

Mitigating Measures

The foundation for eliminating small bribes, Spinelli says, begins with a proper risk assessment to identify where the problematic areas are in your business: What employees are most likely in a position of paying small bribes and facilitation payments? What factors are causing those payments to be made? What controls should the company put in place to mitigate them?

If employees have to pay a small bribe for whatever reason, the company should ensure these payments are recorded, Glass advises. That way, senior management can better assess where potential issues exist, and then they can try to address those issues, he says.

Travel and entertainment expenses are an especially common source of small bribes. Companies may want to consider having a policy in which receipts are required for cash payments over a certain amount, such as $20 or $50, Bailey says, "and ensure that people write a description of what the business purpose was for that payment."

Provide communication and training to employees to make clear the company's policy regarding small bribes and facilitation payments, what to do if they encounter such a situation to pay a bribe, and how to identify what constitutes a bribe. "People may not recognize when something relatively small is a bribe, because what constitutes a bribe can vary depending on the specific circumstances," Bailey says.

"With hindsight, most people will clearly recognize a request for a bribe, but often these things happen very quickly in a high-pressure situation," says Kevin Braine, managing director and head of EMEA for the compliance practice at Kroll. "That's the danger. People have already handed over the $20 before they stop and really think about the consequences." ■

COUNTERING SMALL BRIBES

Below Transparency International outlines several principles for tackling the issue of small bribes.

Effective countering of small bribes, including facilitation payments, should be based on the following principles.

A supporting culture of integrity: A corporate commitment to ethics and integrity provides an enabling environment for countering small bribes and will include integrity expressed in 'tone-from-the-top,' a policy of prohibition of bribery in any form and an effective over-arching anti-bribery program.

Corporate commitment to eliminate small bribes: The company commits to a policy of prohibition of small bribes & a strategy for their elimination through a program of internal controls and collaborative action.

Risk assessment as the basis for designing the strategy and program: The company identifies and assesses the risks that small bribes are demanded or paid in its activities and operations, and the factors that cause them.

The company implements a programme to counter small bribes: A programme of internal controls is implemented comprising detailed policies and procedures to counter small bribes.

Communication and training: As part of the program, communications and training make clear the company's policy of prohibition of small bribes and give requisite information and advice to employees on how to anticipate and resist demands, seek advice and to report concerns or instances of small bribes.

Third-party due diligence: As part of the program, the company has in place appropriate procedures for third parties including due diligence, contract terms, communication, training and monitoring.

Internal accounting controls designed specifically to counter small bribes: As part of the program, the company's internal accounting controls are modified and extended to counter small bribes.

Appropriate actions taken in the event small bribes are detected: As part of the program, the company has a procedure to deal with any incidents including investigation and review, disciplinary action and consideration of reporting the incident to the relevant authorities.

Monitoring the effectiveness of the compliance program to counter small bribes: The program for countering small bribes is regularly monitored and reviewed.

The company acts strategically to influence the corruption environment in which it operates

Source: Transparency International

How Two Companies Got FCPA Charges Dropped

By Jaclyn Jaeger

Often the best guidance on how to avoid Foreign Corrupt Practices Act charges comes from the details of cases that government authorities chose not to pursue. Companies looking to improve their FCPA compliance programs got two such cases recently. Together, the cases speak volumes about how to get a declination from the Department of Justice.

In an unusual move, the Department of Justice opted not to bring enforcement actions against Image Sensing Systems and Layne Christensen in two separate cases pertaining to alleged violations of the FCPA. Statements issued by the companies themselves cite numerous reasons why the Justice Department declined to prosecute.

The decision not to pursue charges of any kind is a marked departure from most FCPA cases, in which the government typically gives companies credit for strong compliance programs, often entering into non-prosecution agreements or deferred prosecution agreements. Even those agreements, however, almost always come with strings attached; it's rare for a company to get complete exoneration.

The most recent case to result in a declination resolved an FCPA investigation into ISS. The developer of traffic management systems first disclosed in a securities filing in March 2013 that law enforcement authorities in Poland had charged two employees of ISS Europe, its Polish subsidiary, with criminal bribery violations related to a project in the country.

. In response, a special subcommittee of the audit committee immediately engaged outside counsel to conduct an internal investigation, and voluntarily disclosed the matter to the Justice Department and the Securities and Exchange Commission, the company stated in a securities filing. In September 2014 both agencies notified the ISS that they would not bring any enforcement actions.

Self-Disclosure

The ISS declined to offer further comment, other than what's already been publically disclosed. In comparison to another FCPA investigation that similarly resulted in a declination by the Justice Department, however, the two cases together highlight the potential benefits companies can gain from voluntary disclosure.

In the second case, for example, global water management, construction, and drilling company Layne Christensen also chose to self-disclose to the government after questions were raised internally in September 2010 concerning potential improper payments that had been made over a considerable period of time by Layne to third parties interacting with government officials in Africa.

Russ Berland, a partner with law firm Stinson Leonard Street, who represented Layne in the investigation, says the company discovered the questionable payments while it was in the process of enhancing its anti-corruption compliance program and in the course of beginning a global risk assessment.

"When those issues came to light, we embarked on an internal investigation," explains Steve Crooke, general counsel of Layne. The audit committee of the board engaged outside counsel and accounting firm BKD to assist in its efforts.

Prior to making the voluntary disclosure, the company first needed to determine "whether the issues that had been raised had enough credibility and substance to be self-disclosed," Berland says. The initial plan was to first look into the original allegations, and then beyond that to determine whether other issues needed to be addressed, he says.

The initial review period lasted two months and involved interview trips to Perth, Australia (where Layne's regional accounting center was located) and Zambia. Based on the results, the board made the decision to self-disclose to the Justice Department and SEC in December 2010.

Following that self-disclosure, the investigation process was extensive, to say the least. The Stinson investigative team, for example, made several on-site visits to numerous company locations in Africa and Australia, where the alleged misconduct occurred or relevant information was kept. This included the Democratic Republic of Congo, Burkina Faso, Mali, Tanzania, and Zambia and Perth.

With the assistance of other Stinson attorneys who were "extremely adept at thorough and economical document review," Berland says, the investigation team at the completion of the investigation had obtained 47 hard drives and 22 mobile devices and had combed through over two million documents.

Cooperation Credit

Cooperation went a long way. Berland says the idea was to approach the government with the mindset, "'this is your area. We'll take whatever direction you give us on how this is done.' At every step, we not only cooperated with the government's requests, but tried to anticipate what they might need," he says. "We found it to be an extremely cooperative relationship."

Since the company chose to self-disclose from the get-go, "we just decided that, no matter what, we were going to continue in that mode of cooperation and transparency," Berland says. "In the end, it served us very well."

In August the Justice Department notified Layne that it had closed its inquiry into the matter, although the SEC's investigation remains ongoing. "We hope to settle the SEC investigation in the near future," Layne's CEO David Brown said in a statement.

Crooke says the Justice Department's resolution of the investigation reflected Layne's "self-disclosure, appropriate remediation activities, and very good cooperation with the government regulators."

Layne's situation also serves as yet another example of the potential tangible monetary benefits that can be gained from voluntary self-disclosure and cooperation. Based on the Justice Department's decision to close its investigation, Layne reduced its previous accrual for resolution of the matter from $10.4 million to $5.1 million.

Kris Tufto, chief executive of the ISS, also stressed the lasting influence of the company's cooperation credit. "From the very beginning, we have voluntarily cooperated with the

authorities and have worked diligently to implement measures to enhance our internal controls and compliance efforts," he said. "We understand that those efforts have been recognized and that the resolution of the investigation reflects this cooperation."

During remarks at the Global Investigation Review Program in 2014, Marshall Miller, principal deputy assistant attorney general for the Justice Department's Criminal Division, reiterated the importance of cooperation. "We would like corporations to cooperate; we will ensure that there are appropriate incentives for corporations to do so," he said. "But if there is no cooperation, we will continue to investigate and prosecute the old-fashioned way, and companies will face the consequences."

"If a corporation wants credit for cooperation, it must engage in comprehensive and timely cooperation," Miller added. "Lip service simply will not do."

In addition to ISS and Layne, other companies that have received declinations, in part, for their cooperation during an FCPA investigation include firearms manufacturer Smith & Wesson, and oil and gas company PetroTiger.

In addition to voluntary disclosure and cooperation efforts, both ISS and Layne also implemented a series of remedial measures to enhance their internal controls and compliance efforts. For its part, ISS said it ended the employment of the two Polish employees involved in the misconduct. "We are also assessing and implementing enhancements to our internal policies, procedures, and controls," the company stated.

With the assistance of Manny Alas and his team at PwC, Layne took "an in-depth evaluation and assessment of its internal controls and compliance practices including the redesign and implementation of new or enhanced FCPA controls and procedures" Berland says. These efforts were led by the company's newly appointed chief compliance officer, Jennafer Watson, to ensure the company put in place best-in-class compliance controls, he says.

Initially, the compliance group focused very heavily on FCPA compliance, particularly in Africa, where the misconduct allegedly occurred, Berland explains. From there, Watson built out the compliance program, which included extensive face-to-face training with third parties in those countries, as well as employees, who were "trained, and trained, and trained again," Berland says.

Layne further instituted "a very robust due diligence program for its third parties," particularly those who have regular interaction with government officials, Berland says. Based on that due diligence, the company made the determination to not continue work with certain third parties, he says.

The company also put in a number of robust compliance controls. Specifically, the company focused on the monitoring and auditing of transactions "to make sure there weren't any dollars flowing out to third parties that had not been vetted and approved," Berland says.

Showing the company's commitment not only to the investigation, but also the remediation efforts is "absolutely essential," Berland says. In the case of Layne, for example, not only did Crooke attend all of the meetings with the government, "but on several occasions, the chair of the audit committee attended, as well," he adds. "That sent a very positive message to the government that the company got it and was doing the right things."

Learning From Morgan Stanley

In 2012, the Justice Department similarly exonerated Morgan Stanley of FCPA charges for its extensive cooperation, robust internal compliance program, and voluntary disclosure of the misconduct. "Often overlooked is one of the critical factors that led to that declination: Morgan Stanley assisted the government in identifying the individual executive responsible for the criminal conduct, Garth Peterson, and in securing evidence to hold Peterson criminally responsible," Miller said.

For other companies facing an FCPA investigation, engaging the help of outside experts who have been through the process many times before and can help the company "not have to reinvent the wheel," Berland says, really helps in the end to see the successful conclusion of an FCPA investigation and remediation. ■

LAYNE'S FORM 10-Q

Below is a statement from Layne Christensen regarding the Justice Dept. and SEC FCPA probe.

As previously reported, in connection with updating its Foreign Corrupt Practices Act policy, questions were raised internally in late September 2010 about, among other things, the legality of certain payments by Layne to agents and other third parties interacting with government officials in certain countries in Africa. The audit committee of the board of directors engaged outside counsel to conduct an internal investigation to review these payments with assistance from outside accounting firms.

The internal investigation found documents and information suggesting that improper payments, which may have violated the FCPA and other local laws, were made over a considerable period of time, by or on behalf of, certain foreign subsidiaries of Layne to third parties interacting with government officials in Africa relating to, among other things, the payment of taxes, the importing of equipment and the employment of expatriates.

Layne made a voluntary disclosure to the U.S. Department of Justice and the Securities and Exchange Commission regarding the results of the investigation and have cooperated with the DOJ and the SEC in connection with their review of the matter. On August 6, 2014, the DOJ notified Layne that inquiry into this matter has been closed. The investigation by the SEC remains ongoing.

Layne is engaged in discussions with the SEC regarding a potential negotiated resolution of these matters. Layne believes that it is likely that any settlement will include both the payment of a civil monetary fine and the disgorgement of any improper benefits.

Source: Layne Christensen

Global Transparency Failures Endure, Adding Risk

CCOs trying to build a robust anti-corruption program often run into a brick wall when confronted with a lack of enforcement transparency from other countries

By Jaclyn Jaeger

One of the great challenges for U.S. compliance officers—who genuinely do want to build robust anti-corruption and anti-money laundering programs worldwide—is the basic lack of transparency into enforcement information in other countries. Two reports might shed a bit more light on the subject.

The reports, one published by Transparency International and the other by Arachnys, examined disclosure practices in numerous countries and found big holes in the availability of enforcement decisions, corporate disclosers, litigation records, and media outlets. That lack of access leaves compliance officers struggling in regulatory darkness as they try to build global programs.

"Getting access to information is not becoming easier," says Adam Foldes, advocacy adviser at Transparency International in Germany and co-author of TI's annual progress report on the member countries to the Organization for Economic Co-operation and Development's Anti-Bribery Convention. According to TI's report, "the availability of information concerning investigations, court cases, judgments, and settlements continues to be a challenge in numerous countries."

Another study conducted by compliance analysis firm Arachnys supports those findings. The Arachnys Open Data Compass index, which examined the public disclosure practices in 215 countries, assessed three aspects of public disclosure transparency:

- Availability of corporate data from corporate registries, stock exchanges, chambers of commerce, and government documents;
- Availability of litigation records from court websites, bar associations, and third-party case law repositories, like the World Legal Information Institute; and
- Development of the country's media environment.

According to the Arachnys index, the United States topped all three areas of public disclosure transparency, with an overall score of 92 out of a possible 100. It fared best in the areas of media and litigation transparency (scores of 99 and 100, respectively), but received a mediocre score of 77 on corporate data.

The United States did not fare as well, however, in TI's progress report on OECD agreements. "In the United States, information from authorities on investigations and on case referrals from and to other countries is not completely available," the report stated.

Specifically, TI said, the Securities and Exchange Commission and the Justice Department currently don't disclose the number of ongoing investigations; when those probes commenced; or whether, when and why the agencies decline to pursue enforcement action.

"While companies listed on securities exchanges may disclose such information to their shareholders in public filings, such disclosures provide an incomplete picture of enforcement activity," the report said. If enforcement agencies published that information themselves, TI continued, that would be valuable guidance for companies about what types of preventative or remedial measures reduce the likelihood of

BOTTOM 10 GLOBAL RANKINGS

Arachnys scored 215 countries and territories based on media environment, provision of official corporate data, and the availability of litigation records. The following 10 companies received the lowest scores.

Rank	Name	Overall Score	News Score	Corporate Score	Litigation Score
206	Palau	13	14	0	25
207	Maldives	13	18	3	18
208	Central African Republic	12	37	0	0
209	South Sudan	12	35	0	0
210	North Korea	11	32	0	0
211	Turkmenistan	10	18	13	0
212	Nauru	10	15	0	14
213	Western Sahara	9	28	0	0
214	Micronesia, Federated States of	8	12	13	0
215	Turks and Caicos	5	14	0	0

Source: Arachnys.

an enforcement action. (To be fair, the Justice Department does occasionally publish public declinations—such as in the cases of Morgan Stanley and PetroTiger.)

> "Not only is a British overseas territory the best place to achieve anonymity, but British assets, specifically London property, are the investment of choice for criminals looking to complete the illusion that dirty money is clean."
>
> David Buxton, CEO & Cofounder, Arachnys

TI made much the same criticism about disclosing more enforcement settlements in its comments about Britain and the U.K. Serious Fraud Office.

In the Arachnys report, Britain ranked No. 2 behind the United States, with an overall score of 83 out of a possible 100. It fared best in the areas of corporate transparency (perfect score of 100), but received scores of 75 and 74 for litigation and media transparency, respectively. Other countries that received high overall scores were Ecuador, France, Albania, and Australia.

Where the findings showed the most improvement is in Latin America, where "quite a lot of new platforms and portals were put online," says Ed Long, head of research for Arachnys. Venezuela, Brazil, and Ecuador "all have made improvements to their public data," Long says.

The impetus behind that, Long says, are probably the high-profile corruption cases going on in the region—particularly in Brazil, where the massive investigation of state-run oil giant Petrobras continues. Greater transparency and disclosure is Latin America's way of demonstrating that "they're trying to tackle their corruption and transparency issue," he says.

Meanwhile, three notorious tax haven islands received the lowest rankings in Arachnys' overall index: Turks and Caicos Islands, Micronesia, and Nauru. Turks and Caicos ranked lowest "due to its complete lack of a public corporate registry, its court records not being available online, and its under-developed news industry," Arachnys said.

"The Turks and Caicos Islands are a black hole for company and legal information, which makes it an extremely attractive place from which to launder money," says David Buxton, CEO and co-founder of Arachnys. "Not only is a British overseas territory the best place to achieve anonymity, but British assets, specifically London property, are the investment of choice for criminals looking to complete the illusion that dirty money is clean."

Enforcement data

Both the Arachnys index and the TI report also noted several countries whose investigations and enforcement data is lagging. "The systematic collection and publication of enforcement data has serious shortcomings," Transparency International said. These countries include Argentina, Brazil, Bulgaria, Colombia, France, Ireland, Japan, Mexico, Portugal, Slovenia, South Korea, and Spain.

In several other countries, statistical data on foreign anti-bribery enforcement is either out of date, such as in Ireland; or missing altogether, such as in Belgium, Greece, and Russia. In Italy, too, "information on foreign bribery-related investigations and cases in over 100 courts is not accessible by the public," TI said in its report.

Disclosure is also lacking in Germany, where authorities keep details on investigations and charges, but never disclose the names of the defendants nor of the countries involved, TI said. In the Arachnys index, Germany received a score of only 43 for litigation disclosure.

In the Arachnys index, Austria is another country that received low ranks for transparency. One reason, Long says, is that much data in the country has been privatized, meaning it must be purchased from third-party providers. That can make it more difficult to obtain, he says.

From a due diligence standpoint, a lack of transparency in enforcement data is concerning. If one company is weighing the acquisition of another, for example, and wants to do a due diligence check, "it's important to know who the potential business partners are, and if they've been implicated in any illegal activities," Foldes says. Investigations and enforcement alone are not enough, he says—"it should be public to have the deterrent effect."

Due Diligence Efforts

In countries where companies have limited access to certain information, compliance and legal executives can try various other sources. For example, in countries where companies have an obligation to disclose regulatory investigations (such as right here in the United States) one helpful source of information is directly from the companies themselves in their disclosure materials, Foldes says.

References are another way to verify not only the quality of a potential business partner's work, but also whether the partner has engaged in any illegal activities. In-depth analyses on country-by-country enforcement actions and investigations—such as those provided by OECD, TI, and Arachnys—are another avenue for information.

Companies can also build safeguards into their contracts with third parties, Foldes says, in the event that a third party cannot fulfill its contractual obligations due to an enforcement action, for example.

A country cannot simply combat bribery and corruption with strong disclosure practices. "It's a long-term cultural change," Long says. "Part of that is transparency. Part of it is enforcement." ■

Auditing Anti-Corruption: Best Practices Emerge

The Justice Department cited 13 action items in recent DPAs as compliance program best practices

by Tammy Whitehouse

As internal auditors stretch into new areas of corporate risk, audit techniques around anti-corruption programs are starting to mature.

Highly regulated companies, or companies that have been stung by some kind of violation of anti-corruption rules, are becoming the pioneers in determining how to satisfy authorities that they are doing all they can to prevent corruption, according to experts who are helping develop new anti-corruption practices for the internal audit profession to model.

"It's a mixed bag out there right now," says Vikas Agarwal, a partner in PwC's risk assurance practice. "There's a large focus by financial services companies and those that are more heavily regulated to have a much stronger anti-corruption program. As you move down, you have multinational companies, technology and software companies, and large retail companies that are very quickly moving up the curve with heightened scrutiny."

Companies are employing a variety of methods and techniques to audit the anti-corruption effort, says Agarwal, beginning with a strong risk assessment and continuing with advanced technology, such as data analytics. "Companies are using data to see what might be an office, a region, or a transaction that they want to scrutinize more," he says.

> "As you move down, you have multinational companies, technology and software companies, and large retail companies that are very quickly moving up the curve with heightened scrutiny."
>
> Vikas Agarwal, Partner, Risk Assurances Practice, PwC

Tom O'Reilly, director of internal audit at technology company Analog Devices, says he's developed a method for auditing the company's anti-corruption efforts by following guidance from the Justice Department found in many deferred-prosecution agreements. It's become something of an audit framework, he says. "It's like a step-by-step guide," he says.

The Department of Justice cites 13 action items in recent DPAs as "corporate compliance program best practices." They cover areas such as a corporate code of conduct, tone at the top, policies and procedures, risk assessments, annual reviews, senior management oversight and reporting, internal controls, training, discipline, ongoing advice and guidance, use of agents and other business partners, contractual compliance, and ongoing assessments.

"This is what a third party, the Department of Justice says, is recommended so you don't have violations in the future," O'Reilly says. "So any auditor who takes this guide and performs an audit using these 13 steps—it's a much more robust audit to provide assurance to the audit committee, the board of directors, and executive management that we've covered all these areas."

Following those 13 steps as an audit framework helps focus attention on specific areas beyond a simple yes-or-no answer to whether specific elements of an anti-corruption program exist, O'Reilly says. "Even though someone says they are doing something, that doesn't mean it's as mature as it could or should be." He focused on training as an example. The company may provide a once-a-year online training module for employees, but what else is done to support it? "What else can we do?" he asks.

Sanglier

Raytheon Co. asked itself that question when it faced problems with FCPA compliance in the late 2000s. Tom Sanglier, director of internal audit at Raytheon, says that experience sparked management to "up its game" around anti-corruption efforts. The company formed a cross-functional task force that meets weekly to review the program and improvement initiatives. The company makes extensive use of data analytics, he says, to review transactions and communications, looking for red flags that warrant further inquiry.

"We do a lot of transaction monitoring, depending on the risks," Sanglier says. "We use data analytics to make sure we're looking not just at dollar amounts, but also keyword searches to identify any potentially corrupt transactions. We also put our reps and consultants through an extensive due diligence process."

Internal audit's role, Sanglier says, includes traveling to up to a dozen international locations to perform on-site reviews and transaction testing, meeting with selected representatives and consultants, and questioning them directly about their understanding of the company's policies on bribery and corruption. His staff also performs select audits at the enterprise level to examine how the overall process is functioning.

Auditing an anti-corruption program is much like auditing other functional areas of the business, says Bill Henderson, a partner in fraud investigation and dispute services for EY—namely, that it begins with an assessment of risk. "Generally, what you're doing is taking a risk-based approach and looking at where the greatest corruption risks are for the company," he says. "Those are the risks you focus on in doing your audit procedures."

> "[A]ny auditor who takes this guide and performs an audit using these 13 steps—it's a much more robust audit to provide assurance to the audit committee, the board of directors, and executive management that we've covered all these areas."
>
> Tom O'Reilly, Director of Internal Audit, Analog Devices

Companies at greater risk for corruption tend to be more active in auditing their programs, Henderson says. Companies with heavy overseas operations, or those in higher-risk industries (defense, oil and gas, telecommunications, and the like), are more likely to be auditing their anti-corruption programs. "This is an area that lends itself to monitoring and auditing as being an important part of the program," he says.

Jeff Maimon, a partner in advisory services at EY, says the adoption of the 2013 COSO Internal Control-Integrated Framework has led companies to take a closer look at what they are doing to prevent and detect fraud, which then is leading some to consider what more they can do to audit those efforts. "Do we have sufficient programs, processes, and procedures to both prevent and detect corruption and fraud?" he says.

In addition, many internal audit shops across the profession are being asked (as always) "to do more with less," Maimon says. That has inspired some internal audit shops to assure they are not operating in that second line of defense as defined by the Institute of Internal Auditors, where risk functions are overseen. Instead, some internal auditors are looking to provide assurance about the anti-corruption effort rather than hold responsibility for directly overseeing it, he says.

In Henderson's view, the Justice Department guidance contained in deferred-prosecution agreements is a reasonable starting point, encompassing elements that should be present (and therefore audited) in any anti-corruption program. The firm likes to point companies to the resource guide on the Foreign Corrupt Practices Act published jointly by the Justice Department and Securities and Exchange Commission as a starting point for planning an internal audit, he says.

"It's a lot of the same information," he says. "Those are the leading practices." ■

ANTI-CORRUPTION INTERNAL AUDITS

The following is an excerpt from EY's anti-corruption compliance report.

Creating an effective anti-corruption audit program requires having the right people, processes, and technology. Anti-corruption audits are very different from other internal audits usually conducted by a company's internal audit group. The auditors need to be trained in the particulars of the FCPA, the U.K. Bribery Act, and local anti-bribery laws. It is also useful to have an understanding of leading compliance practices related to these laws. Core skill sets beneficial to have on the audit team include: good interviewing skills, the knowledge and experience necessary to select high-risk transactions for testing and to recognize red ags, indicating potential violations. Some companies choose to have their internal audit department conduct these audits. Others employ different strategies—pairing legal or compliance department personnel with internal auditors or using outside forensic accountants.

Key reasons for using experienced forensic accountants include the ability to select meaningful transactions for review and experience in recognizing corruption red flags. An experienced forensic accountant who understands the FCPA and U.K. Bribery Act and has been involved in corruption investigations and anti-corruption audits, applies technical knowledge, experience, and seasoned judgment in selecting testing samples and reviewing transactions. Knowing where to look is an important intangible factor that greatly increases the value of the exercise. A random sampling selection will offer limited opportunity to detect and therefore deter potentially problematic transactions. Corruption investigation experience is required to understand, when you get into certain areas, how far back you need to probe or "peel the onion." This is where an inexperienced financial auditor often struggles.

Anti-corruption audits are preferably stand-alone audits that are not integrated into a larger set of procedures. Generally integrating anti-corruption audit procedures into larger audit programs is not the most effective practice; it commonly leads to situations where the auditor doing the testing lacks the necessary training and experience, focus, supervision, or time to do the work properly. To avoid "audit fatigue" commonly expressed by business units, the timing can coincide with an internal audit of the same business unit but the activity should remain separate.

In conducting substantive testing, the purpose is to identify potential corruption violations or red flags. The audit is not an investigation. It is a business process like other internal audits a company might undertake—a predetermined set of procedures designed to assess corruption risk and test for compliance with company policies. Serious violations or red flags uncovered in the audits are typically reported to legal or compliance professionals for further investigation. Protocols should be put in place for immediate consultation when a potential violation is uncovered. Often such audits are conducted at the direction of a company's general counsel and are subject to the attorney-client privilege.

Source: EY

Q&A: How PetroTiger Avoided FCPA Prosecution

Sidley Austin Partner Timothy Treanor discusses PetroTiger's win

by Jaclyn Jaeger

As part of our occasional series of conversations with voices in the compliance world, we caught up with Timothy Treanor, a partner with law firm Sidley Austin who represented oil and gas company PetroTiger. In 2015, PetroTiger became just the second company in recent history of the Foreign Corrupt Practices Act (after Morgan Stanley in 2012) to avoid prosecution by the Justice Department, despite guilty pleas by three of its top executives. Treanor provides insight into how PetroTiger escaped charges.

Typically when the Justice Department brings FCPA charges against a company's executives, charges against the company itself aren't far behind. The Justice Department's rare declination followed a guilty plea by Joseph Sigelman, the former co-chief executive officer of PetroTiger, for conspiring to pay bribes to a foreign government official in violation of the FCPA.

At his plea hearing, Sigelman admitted to conspiring with co-CEO Knut Hammarskjold, PetroTiger's former general counsel Gregory Weisman, and others to make illegal payments of $333,500 to David Duran, an employee of the Colombian national oil company, Ecopetrol. Sigelman admitted to making the payments in exchange for Duran's assistance in securing a $45 million oil services contract for PetroTiger.

Treanor

Sigelman was the third former PetroTiger executive to plead guilty in the case. In 2013, Weisman pleaded guilty to conspiracy to violate the FCPA and to commit wire fraud. In 2014, Hammarskjold pleaded guilty to similar charges.

What corporate defense strategies proved most effective during the negotiation process?

We were able to show that the three convicted executives were not fully disclosing the financial condition of the firm to the board. They changed the budget without board authorization. They did a number of different things to deceive the board.

We were also able to show through evidence that board members were not just sitting by, letting the executives run amok. From the very beginning, they imposed a stringent business Code of Conduct. They responded to issues that arose and had not turned a blind eye.

When they heard rumors of potential misconduct, they interviewed employees to try to understand if there were integrity issues that needed to be addressed. This led to one of the board members being banned from company premises by one of the executives, because he believed that the board member was interfering with the operation of the company. E-mails retained by the company substantiated that claim, and we presented it through the evidence. The board also fought to bring in forensic accountants to take a look at financial transactions within the firm. That didn't happen, in part because the executives didn't allow it to happen, but the effort was there.

The board was very aggressive about upholding high standards of integrity. They were doing all the things that the government would want to see board members doing.

What actions did the board take after discovering the misconduct that the Department of Justice looked upon most favorably?

After finding out about the misconduct, the board was quick to remediate any deficiencies that they uncovered. They enhanced financial controls and other compliance controls and did a full review of their policies and procedures. They had the executive management team attend specific trainings, and we were able to show that to the government as well. I think that proved to be very helpful to the company.

They went so far as to push [the culpable executives] out of the company and bought back their shares. Given that these executives were substantial shareholders of the company, that's a pretty drastic move to push them out and get them to sell back their shares By doing so, that ultimately led to our second—and maybe our strongest—argument, which was that, "If you punish the company, you're only punishing the good guys and heaping more victimization upon them. To punish them would be unfair." We were persistent in our argument.

> We were able to show that the three convicted executives were not fully disclosing the financial condition of the firm to the board. They changed the budget without board authorization. They did a number of different things to deceive the board.

How responsive was the Justice Department in accepting that argument?

The Department initially was surprised that we would ask for such a resolution in a case like this, in which senior executives were implicated. They told me it was an aggressive request, but to their credit they listened.

I think it would have been very easy for them to say,

I know the Department of Justice has not been willing to draw a line and say, "If you self-disclose, you're eligible for a declination. If you don't, you're not." They're not that black and white. To me, however, if you don't self-disclose, you're at a significant disadvantage in getting a declination.

"Listen, you have two CEOs and a general counsel who have been implicated. There is no way we're letting the company off without some sort of punishment that we can show for this conduct." But they worked through our arguments and talked about alternatives and what that would mean for the company. It was a fairly extensive discussion over a period of months.

How much of a factor did PetroTiger's voluntary disclosure of the misconduct play into the Justice Department deciding not to prosecute the company?

I think that was a huge consideration. I know the Department of Justice has not been willing to draw a line and say, "If you self-disclose, you're eligible for a declination. If you don't, you're not." They're not that black and white. To me, however, if you don't self-disclose—if the government finds out about the misconduct on its own—you're at a significant disadvantage in getting a declination. The fact that PetroTiger came forward was a big plus.

What broader lessons can other companies take away from PetroTiger's case?

One of the key factors that the Department of Justice considers when determining the severity of an FCPA violation is whether any senior executives were involved in the misconduct. In this case, you have the two co-CEOs who were convicted, and the general counsel who was convicted, of participating in FCPA offenses.

Nonetheless, the company received a declination. So for others out there it shows that under the right circumstances you can, perhaps, get a favorable resolution in an FCPA matter, even in a case in which senior executives were involved. When you have a board in which the outside directors are doing everything right, that that can be a defense.

It pushes the boundaries of the types of cases that are eligible for a declination.

What parting words would you leave with other companies that are facing an investigation for violations of the Foreign Corrupt Practices Act?

The dialogue, and the tone of the dialogue, is very important. You have to establish the government's confidence in you. You have to establish that the investigation you've done, and the facts you have uncovered, have integrity—that that process was an appropriate process, and that they can rely upon what you're telling them.

The government will come to you with a skeptical eye, looking for signs that they should not be relying upon your work, and you have to pass their scrutiny. We got through that process, I believe very successfully, because we had cast a wide net when we were looking for facts, and we had been very aggressive in our search.

When you get a declination, you say, "Thank you," and you don't ask a lot of questions. ■

ABOUT TIMOTHY TREANOR

Below is a brief biography for Timothy treanor, a partner with law firm Sidley Austin, who represented PetroTiger against FCPA charges.

Timothy Treanor is a partner and global co-leader of the white-collar criminal defense and investigations practice group at Sidley. He is also a former federal prosecutor who represents companies and individuals in investigations, enforcement actions, and prosecutions conducted by various government agencies, including the U.S. Department of Justice, the Securities and Exchange Commission, and the New York Attorney General's Office, and he frequently manages parallel criminal and civil proceedings and global investigations involving enforcement agencies in multiple countries.

Corporate clients he represents include leading companies in a variety of industries, including financial services, pharmaceuticals, insurance, oil and energy, and technology.

Treanor also advises companies on the development of internal compliance programs and provides compliance counseling on a host of criminal issues, including the Foreign Corrupt Practices Act, anti-money laundering, sanctions, fraud detection, anti-counterfeiting, and internet gambling issues.

Treanor has extensive experience working with corporate compliance monitors. He currently serves as lead counsel to the Monitor of HSBC Holdings and its subsidiaries appointed by the Justice Department, the U.K. Financial Conduct Authority, and the Board of Governors of the Federal Reserve System, in connection with HSBC's $1.9 billion resolution of money laundering and sanctions violations.

As a federal prosecutor, Treanor selected and managed a corporate compliance monitor for a corporate defendant and advised on the Justice Department's Guidelines for selecting and using monitors.

Technology Gives Teeth to an Anti-Corruption Program

Why it's high time to move beyond spreadsheets and shared folders

By John Verver, CPA CA, CISA, CMC, Strategic Advisor to ACL

There are many components to an effective anti-bribery and corruption program. Tone (and real commitment) at the top, as well as policies, training, communication, risk assessment, and monitoring all have important roles to play. Doing a good job in organizing people and processes around these components is essential. What about technology? It's a given that no anti-corruption program is going to work without any use of technology. The questions to consider in order to create a really successful anti-corruption program include: which technologies, where to apply them, and how?

In the earlier days of implementing GRC-related programs, including anti-corruption, it was common practice to assume that spreadsheets, email, Word documents and shared folders were a workable solution. Most organizations who took this route now know that this can be a frustrating and unreliable path. It is now generally accepted that a wise choice in selecting software designed specifically for risk management, compliance and audit is a good investment and can have a hugely beneficial impact, both on reducing the burden of compliance activities and on making them more effective.

Have you considered these important application areas?

Many aspects of an anti-corruption program are relatively straightforward, such as documenting policies and communicating them. But simply letting people know what they should be doing is the relatively easy part. The larger challenges come in determining whether the policies are actually effective—and what should be done to make them better. Implementing technology just to pay lip service to compliance requirements is not solving the problem. There are a number of areas in which technology can make a particular difference:

1. Initial identification and assessment of risks and controls

As with any compliance program, the smart approach involves understanding and assessment of risks. The focus of efforts can then be on areas of higher risk. What's the point of investing large amounts of efforts on policies and controls in areas where actual risks are very low?

The problem is that it is not always obvious where the real risks lie. But there has to be an initial place to start and this means building a repository of potential risks—all the things that could lead to non-compliance with anti-corruption legislation and risks such as reputational damage, regulatory authority prosecution, and penalties.

After identifying potential risks, the next stage is to determine what policies and controls should be in place to reduce the risks. After an initial assessment of risks and corresponding controls it should be possible to produce an overview of the current state of risks arising from bribery and corruption. This is often presented in a visual format, using some form of "heat map" to illustrate the areas of greatest concern.

Most risk management and compliance technologies are designed to support the process of developing and managing a risk and controls repository. Some technologies also do a very good job in managing surveys, questionnaires, self-assessments, and sign-offs—providing an important link to what is happening in the field. These response-based "human analytics" provide indications of how seriously people are taking their responsibilities around corruption policies. Responses can be analyzed and reports generated that often provide early warnings of where issues are likely to arise.

2. A dynamic ongoing approach to risks and controls

Risk assessment is not a one-off process. Initial identification of risks and controls is just the starting point. How do you know whether the controls are working? Are there risks that have not yet been identified?

Technology plays an obvious important role in simplifying the process of documenting risks and controls related to bribery and corruption. But where it really delivers a unique benefit is in the ability of data monitoring, testing, and analysis software to determine whether the controls that are meant to be in place are actually effective. Data analysis software also provides insights into whether there are new risks for which no controls have been implemented.

A technology-driven approach to corruption risk and control management is a dynamic one, hot on the trail of emerging risks. As actual compliance failures and weaknesses are identified, procedures and controls can be modified accordingly. Individual instances of apparent bribes get an immediate response and each problem can be addressed before it escalates and turns into a major exposure. And on an ongoing basis, senior management can see up-to-date dashboards that assess and quantify the current extent of compliance risks and control issue.

3. Diving deeper into monitoring

Data analysis is well proven in the world of internal and external audit with its powerful ability to examine very large populations of financial and business activities. It is used to test the effectiveness of controls, as well as to find instances of fraud, error, waste, and abuse. These capabilities are equally applicable to compliance and, specifically, to finding instances of corruption and bribery—and weaknesses in related controls.

Here are just a few examples of analytic tests that organizations typically deploy to detect and monitor for instances of bribery and corruption:

» Matching names of individuals to whom payments are made or other benefits provided with names in Politically Exposed Persons (PEP) or OFAC sanctioned providers databases

» Payments and other transactions in which suspicious wording or descriptions are used

» Unusual or suspect transactions in high risk regions and involving high risk entities

» Payments initiated/approved by managers or individuals deemed likely to be under pressure to be involved in corrupt activities

» Payments made through unusual and potentially high risk bank accounts

Some analytic tests which are frequently used for identification of various fraud indicators are equally applicable for detecting corrupt payments and activities in which there is an attempt to bypass usual control procedures, such as:

» "Flip flop" short duration changes to bank account numbers and/or payee names within the vendor application system

» Vendor data changes and payments approved by unauthorized employees

» Purchase and payment approvals that are "split" into multiple transaction just under an approver's authorization limit

While data analysis can be very effective at testing individual transactions and "finding the needle in a haystack," it is also well suited to providing a quantified overview of the status of monitoring activities. For example, a dashboard can show that over a given time period, $X billion of transactions were tested, resulting in $Y million of suspect transactions that were investigated, and $Z hundred thousand of transactions that were found to be instances of actual corrupt payments. This, in turn, leads to an updated risk assessment analysis, together with accompanying details of the response to the control weakness that allowed the payments to occur.

4. Monitoring and management of red flags

While these forms of analytics can be used to look back at payments and other benefits provided over a substantial period of time, the greatest impact is obtained when data analysis monitoring is performed automatically on an ongoing basis.

This means that indicators of risky transactions and other "red flags" or anomalies are identified in a short timeframe in which there can be an immediate response. While data analysis technology can be highly effective in this process, the reality is that not every flagged exception or anomaly is an actual instance of bribery; some form of review and investigation process needs to take place.

Technology plays a key role in making the exception management process workable. It typically involves automated workflow in which responsibility for investigation is assigned to an individual, and escalated to more senior management if a satisfactory response and resolution fails to occur. Management dashboards again provide an up-to-date overview of the status of the entire monitoring and exception management process.

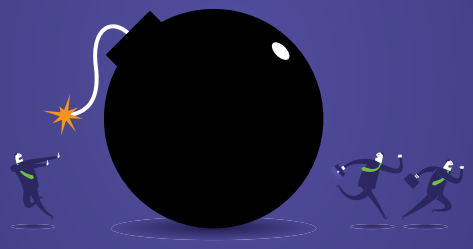
5. Integration with broader risk management and audit

One other area to consider in selecting anti-bribery compliance software is the ability to integrate with broader organizational risk management and audit technology. Using a common technology platform across other related functional areas not only often makes economic sense, but also makes it easier to put bribery and corruption risk management directly in the context of organizational risk management overall.

This does not mean that corruption compliance software can only be implemented as part of an enterprise-wide initiative, which easily results in a failed attempt to "boil the ocean." But it does mean that there can be certain consistency that makes it easier to bring various risk, compliance and audit silos together when needed, as well as to share data (and de-duplicate effort) when it makes sense to do so.

Technology to enable and strengthen processes

In many business areas, technology is not only a vital leg of the "people, process, and technology" stool, but also has been proven to be transformative. Just look at the worlds of banking, brokerage and finance, or retail sales, as examples. For some organizations, technology is already transforming risk management and compliance processes. Applying similar technology techniques to anti-bribery and corruption should only help to transform and reduce the costs and risk exposures in these processes. ■



Let's stay out of the headlines

Are you tasked with safeguarding your organization? Ineffective and inept internal investigations can be very costly to your bottom line AND reputation.

ACL's comprehensive compliance platform reduces the burden of compliance with a data-driven approach to managing end-to-end compliance processes. Streamline and strengthen your compliance program for regulations such as SOX, FCPA, OFAC, or industry requirements like HIPAA, PCI DDS, Dodd Frank, OMB A-123, AML, or internal governance areas like ITGC, ISO, COBIT, self-assessment and policy certification and attestation.

ACL's Compliance Management Solution helps you:

- Reduce the burden of compliance workload
- Map regulatory requirements to your control framework
- Validate internal controls effectiveness
- Prevent reputation damage and fines
- Streamline policy attestation
- Identify, remediate and track issues

acl™

Visit acl.com/Compliance-Management to learn more about taking a centralized approach to compliance management.