Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

New Risks, Strategies in the

Fight Against Corruption

An e-Book publication sponsored by BDO THE Network Integrated GRC Solutions

"Not just global resources. Credibility with the regulators."

People who know Global Forensics, know BDO.

Forensic Accounting at BDO

From fraud prevention to forensic technology, you need a strategic advisor with agility, credibility, and experience. BDO provides compliance, due diligence, and investigative services to clients throughout the United States and around the world. Our dedicated professionals draw on deep experience across a wide range of industries, providing rapid, strategic guidance through even the most challenging of environments.

Accountants and Consultants
www.bdoconsulting.com

Inside this e-Book:

BDO Global Forensics

Serving multinational clients through a global network of more than 1,200 offices in 144 countries, BDO's global forensics professionals assist organizations and their counsel to address cross-border and complex matters involving the risks associated with fraud and corruption, as well as a range of litigation and dispute advisory services.

Global Risk & Investigations
BDO's forensic accounting professionals combine experience and investigative skill to identify, preserve and host relevant evidence, as well as conduct computer forensics and analyze books and records. We assist counsel in interviews on financial and accounting-related matters, and perform background due diligence on individuals or entities of interest, as well as due diligence on potential M&A targets. To help prevent, deter and detect fraud, BDO provides risk assessments, internal controls testing and monitoring.

Litigation & Dispute Advisory
BDO assists counsel on a wide range of multi-jurisdictional disputes, combining our accounting, audit and industry expertise. We provide valuable insight and credible testimony in all phases of litigation, from discovery through trial, and at arbitration tribunals around the world. Understanding how to effectively translate accounting and quantum issues for court or tribunal, we analyze complex financial issues and quantify damages. BDO also provides opinions on financial reporting standards and matters involving accountants' liability.

Forensic Technology Services
Leveraging state-of-the-art technology in our dedicated forensics labs, BDO assists clients with the complexities of electronically stored information. Providing computer forensics, e-discovery and data analytics, we work with clients to obtain, evaluate and report on relevant information, delivering insights to our clients to enable them to make informed decisions. Our technology specialists work on matters large and small, from imaging a few hard drives to processing millions of records spanning international borders in multiple languages.

The Network, Inc. is a leading provider of integrated governance, risk and compliance (GRC) solutions that enable organizations to mitigate risk, achieve compliance, and ultimately, create better, more ethical workplaces. Combining dynamic SaaS-based technology with expert-level services, The Network helps companies around the world protect themselves from the risks posed by fraud and unethical conduct, detect issues early, and correct unethical or illegal behavior.

The Network's integrated solutions include customized programs for confidential reporting of incidents; engaging awareness & communications programs; interactive, expert-level e-learning courseware; collaborative, end-to-end policy management; centralized incident and issue management; enterprise-level process management for corrective action/preventative activities and proactive evaluation of potential compliance-related risks; and an unmatched level of customer service and quality assurance. The company's proprietary GRC platform includes advanced reporting and analytics and a collaborative, intuitive user interface leveraging social media-style controls.

The company's award-winning technology, state-of-the-art contact center, and commitment to their clients' success have made The Network the leading provider of comprehensive GRC solutions. Established in 1982, The Network serves thousands of organizations in every industry, including nearly half of the Fortune 500. More than 27 million employees worldwide rely on The Network. For more information, visit www.tnwinc.com.

Anti-Bribery Efforts Turning to Technology

By Dann Anthony Maurno

The Justice Department and the Securities and Exchange Commission released their "Resource Guide to the Foreign Corrupt Practices Act" more than six months ago, and compliance executives have been poring over its 120-plus pages of case studies and "what not to do" advice ever since.

Nowhere in the guide, however, will you find the words "software" or "analytics."

Still, practical solutions for today's data-centric, globally extended enterprise are what companies need if they are expected to oversee thousands of third parties (or more) and tens of thousands of employees (or more) around the world. So where to begin?

"I would start by asking, 'What's the state of your compliance program?' Do you have a written procedure?" says Tom Fox, an independent FCPA compliance consultant who maintains the FCPA Compliance and Ethics Blog. "If so, then there are four components that can assist you."

Fox describes four general categories, beginning with process solutions that are the overall control system for any FCPA compliance program. These are typically suites of solutions such as those from ACL or The Network. Others are point solutions for specific functions, including transaction monitoring, third-party continuous monitoring, and e-mail and communications relationship monitoring.

Process solutions set the tone for FCPA compliance, reminding employees continuously that checks are in place. Among the process solutions are The Network's FCPA offering, which integrates its GRC suite with policy management, training, and awareness materials. The Network's policy management functionality acts as a central repository for employees to find and attest to policies—acting as a sort-of Google Docs for FCPA policies, which captures signatures and approvals and manages group interactions. GRC suites also include functions such as reporting, incident management, and workflows for managing investigations from allegation through resolution.

GRC suites are where internal controls typically reside. A company can decide, for example, that the compliance department or another oversight group must approve every gift exceeding $400 or entertainment expense more than $150, and use the GRC suite for submissions and approvals.

NAVEX Global is another suite of solutions and services including case management, policy management, online training, and third-party whistleblower hotlines. Third-party hotlines offer a comfort level to employees who may be reluctant to "raise hell" with managers within the organization. They also provide resources and functionality that most companies would be hard pressed to assemble on their own: NAVEX, for example, offers interpretation and translation in 125 languages, and around-the-clock monitoring.

The purpose of process solutions is not just to enforce FCPA compliance policies, but to automate and simplify them. "I think 99.9 percent of the time, someone doesn't know the right process to follow," says Jeffrey Spalding, assistant general counsel at Halliburton. "It's not ill intent—although that does happen and those are the people we need to get rid of—but most of the time it's letting employees know our practices and giving them tools to follow them."

Halliburton is rolling out an automated gift and entertainment control function that requires employees fill out request forms that route through the company's compliance group for approval or denial. Halliburton's policy is that all gifts to non-U.S. government officials require approval by its compliance department (and, as the value rises, by regional management, general counsel, and ultimately by the CEO). Similar procedures exist for bringing non-U.S. government delegations to Halliburton facilities.

"The mantra I preach is, you can have as many policies as you want and automated procedures, but if the employee don't know about them, they are pretty worthless," Spalding says.

All that said, such systems are worth little if they don't help the company win credit with regulators when a violation *does* occur. Proving that employees should have been aware of the company's anti-bribery program can mean the difference between a painful FCPA prosecution and a slap on the wrist or less.

Documentation, for example, spared Morgan Stanley from a hefty fine in 2012 when a former managing director pleaded guilty to conspiring to evade Morgan Stanley's internal accounting controls for FCPA compliance. The company proved that it had trained the manager on FCPA seven times from 2002 to 2008, issued him more than 35 reminders about compliance, and required him annually to certify compliance with the company's code of conduct. The robust, tech-laden systems in place at Morgan Stanley aided the company's efforts to recreate a digital trail of compliance efforts with Peterson.

These Needles Find You

Proving that an employee was trained on anti-bribery policies after the fact is nice; actually finding the behavior and stopping it in its tracks is better. That is where transaction monitoring systems, offering visibility into financial and operational transactions, can enter the picture. They use Big Data analytics to flag items that need attention: say, gifts exceeding $150, uncategorized expenses, or unusual spending patterns in a business unit. With the right parameters, cross-checks, and red flags, instead of finding the proverbial needle in a haystack, the needle finds you.

Among the market leaders is Oversight Systems with its

Continuous Transaction Analysis platform, which in turn integrates with major enterprise platforms like SAP and Oracle. Both SAP and Oracle offer transaction monitoring capabilities of their own, but they do not integrate with one another—and most multinational companies will have more than one financial reporting system, as will companies after a merger or acquisition. That gives smaller vendors like Oversight their business opportunity.

Third-party monitoring and vendor screening services help companies check their vendors and partners against, for example, databases of non-U.S. government officials and Transparency International's Corruption Perception Index. World Compliance maintains the NEO service, which daily checks a client's vendor network against the Global Foreign Official List, a database of state-owned companies, foreign officials, known family members of political figures, and companies owned by politicians. NEO acts as a clearinghouse, on which vendors and partners worldwide register for continuous evaluation as the database is maintained. Kroll Advisory and other firms perform similar services as well.

Companies such as Catelas offer e-mail and communications relationship monitoring. Catelas offers "relationship forensics" to discover who talks to whom, when they connect, and how well they know one another. Global business advisory firm FTI Consulting offers its proprietary Ringtail e-discovery software, designed to simplify e-discovery by looking for "concepts" in documents and correspondence, then putting concepts into visually easy clusters.

As Fox describes, "You may be looking for an employee who sends 10 e-mails to a Gmail account, each with an attachment, and that can be a red flag. Or maybe it's a sales person sending e-mails to someone in the supply chain, when there's no reason for sales to be e-mailing the supply chain. That's relationship monitoring."

Computer Forensics

Still another set of tools includes Forensic Toolkit and EnCase, which combat destruction of evidence by taking a "snapshot" of a given computer in a forensically sound manner. These tools perform a bit-by-bit image of a hard drive beyond the documents to determine whether the user has deleted items, attached a thumb drive, or reinstalled the operating system.

"The key is, who's operating the tools?" asks Martin Weinstein, a partner at law firm Willkie Farr & Gallagher, and coauthor of The Foreign Corrupt Practices Act: Compliance, Investigations, and Enforcement. "You need in FCPA compliance, more than other areas, extremely experienced people who have seen a lot of different patterns, and who know what to pick up on and what not to. A Harvard degree is no substitute for having the experience to discern between the two. It's an art more than a science." ■

FCPA BECOMES SOP

Below are some results from the Kroll Advisory Services 2012 Global Fraud Survey, which explains how many companies adjusted their risk assessments due to U.K. Bribery Act and U.S. Foreign Corrupt Practices Act Enforcement.

In 2012, the Kroll Advisory Services Global Fraud Survey found that the number of senior executives who claimed a thorough assessment of risks arising from U.S. FCPA or the U.K. Bribery Act doubled to more than half of those executives (from 26 percent in 2011 to 52 percent).

More than half of those companies in 2012 had trained their senior managers, vendors, and foreign employees in compliance as well (55 percent versus 29 percent in 2011).

Exactly half claimed that when entering a joint venture, making an acquisition or providing financing, their due diligence includes a review of FCPA/U.K. Bribery Act risks, up from 26 percent in 2011.

According to the Kroll report, there is room for improvement. More than 20 percent of respondents said that although they are subject to the U.K. Bribery Act or U.S. FCPA, they have not made a thorough risk assessment, trained the right people, or amended their due diligence processes.

The Annual Global Fraud Survey was commissioned by Kroll Advisory Solutions and executed by the Economist Intelligence Unit, which polled 839 senior executives worldwide, and from a broad array of industries and functions. Some 53 percent of respondents were C-level, and 52 percent from companies with annual revenues over $500 million.

—Dann Maurno

Percentage of Companies Agreeing With the Following

	2012	2011
We have made a thorough assessment of risks to our organization arising from the U.K. Bribery Act and/or U.S. FCPA and their enforcement, and set in place a monitoring and reporting system to assess risks on an ongoing basis.	52%	26%
We have trained our senior managers, vendors, and foreign employees to become familiar and compliant with the U.K. Bribery Act and/or U.S. FCPA.	55%	29%
When entering into a joint venture, making an acquisition or providing financing, our due diligence includes a review of U.K. Bribery Act and/or U.S. FCPA risks.	50%	26%
Our internal compliance regime isbecoming more global because of the extraterritorial reach of the U.K. Bribery Act and/or U.S. FCPA	56%	26%

Source: Kroll.

Internal Audit's Bigger Role in FCPA Compliance

By Jaclyn Jaeger

As companies continue to push into global markets and regulators intensify scrutiny of risk-management practices, internal auditors are playing a greater role in evaluating and mitigating bribery and corruption risks.

"Bribery and corruption are top risks for many companies," says Princy Jain, a partner in PwC's risk assurance practice. Because of the regulatory focus on anti-corruption and more companies expanding globally, "we've seen greater need over the last couple of years for involving internal audit in the anti-corruption compliance process," he says.

Regulators have noticed that need, too. The Justice Department and the Securities and Exchange Commission have turned up the heat on internal auditors when it comes to their role—or lack thereof—in anti-corruption compliance programs.

In the past, one of the first questions asked by regulators when a fraud was uncovered was, "where were the outside auditors?" says Raymond Sloane, a director at consulting firm Berkeley Research Group. "More frequently that question is now coupled with, 'where were the internal auditors? Why didn't they catch this?'"

Where internal audit can add the most value to anti-corruption compliance programs, say risk-management experts, is on the front-end by helping senior management establish the risk-assessment process at a strategic level.

Specifically, internal audit can aid executive management in identifying and prioritizing the risk areas that need the most attention, the likelihood and significance of those risks, and how to go about designing an anti-corruption program that is proportionate to the company's risk appetite and business strategy, says Stephen Arietta, vice president of internal audit for United Online.

"Internal audit is in a unique position to have visibility into the various operations of a company," Arietta says. "So when you're assessing corruption risks, internal audit can really lead the facilitation process for the conversations being held with senior management."


Arietta

Still, internal audit will have to make some adjustments to transition to assessing bribery risks. For example, the amount of the bribes may not always be material, a key consideration in traditional auditing, but could still present a potential violation, says Sloane. Thus, the cost of an investigation into potential improper payments could be disproportionate to the amount of the alleged payments, "so what we see are companies enhancing their audits in these areas," he says.

> "Internal audit is in a unique position to have visibility into the various operations of a company. So when you're assessing corruption risks, internal audit can really lead the facilitation process for the conversations being held with executive management."
>
> Stephen Arietta, VP of Internal Audit, United Online

"The more you can do up front and the better a job you can do with your training and communication, the better off you're going to be in the long-run," says Charlie Wright, vice president of internal audit at Devon Energy. "It's all about being proactive and setting up processes and procedures and training and communication—making sure all those things are in place."

Compliance & Internal Audit Teaming Up

Because every company has its own unique structure and culture, the role of the internal audit function differs significantly from company to company. At some companies, for example, internal audit works directly with the risk-management team.

At Ryder System, internal audit co-chairs the enterprise risk-management program with the compliance group, "and we use that as an offshoot for our audit plan for the year," says Cliff Zoller, senior vice president of audit services for Ryder. Compliance and audit also jointly train both employees and third-party agents in their local countries on the company's code of ethics and on acceptable behavior, he says.

At Devon Energy, the compliance group establishes the compliance program and internal audit reviews the operating units to ensure compliance with the company's policies. "We're in a little bit of a unique situation at Devon because we've recently divested most of our international properties to be able to invest more in our North American operations," Wright says.

The internal audit function also adds significant value in helping their companies monitor compliance with anti-corruption compliance programs, whether that involves "performing certain audits in certain countries, or looking

at certain data trends on a periodic or continuous basis," Jain says.

At Ryder, for example, internal audit spends roughly 25 percent of its time on continuous auditing of the locations of its largest operations, says Zoller. On a quarterly basis, internal audit requests to see a listing of all accounts payable activities that took place in those countries, which are then closely scrutinized for any potential type of facilitation payment, he says.


Zoller

"You can't look at every transaction; it has to be a risk-based approach based on areas of the world where the company operates," says Sloane. What the regulators want to see is that the testing of the program by the internal audit function is focusing on those areas most vulnerable to bribery and corruption, he says.

In the event that a violation is discovered, internal audit must alert senior mangagement or "report it directly to the audit committee or board of directors," says Sloane.

In the event of an investigation, internal audit needs to keep in mind that their reports are going to be closely scrutinized, "so it's important that if issues arise they see them through to their logical conclusion," says Sloane. "They need to make sure they're identifying red flags that represent potential corruption areas and are following up."

A robust internal audit function will consistently monitor management's remediation efforts on any weaknesses and follow up on their status. Internal audit should "remain independent from the implementation of any of those remediation efforts, but reviewing it and assessing it from a design perspective is appropriate," says Arietta.

In the event of a government investigation, internal audit can help identify issues, accumulate data for the government, and identify whom to interview. Collaboration is an important component of any investigation related to corruption issues, ensuring that "each subject matter expert play their particular role," says Zoller.

Because allegations of bribery and corruption are particularly sensitive, internal audit has to be objective in their review, says Jain. "They have to take into consideration all facts and circumstances."

In any investigation, issues of attorney-client and work-product privilege must be carefully considered also. "It's important, where internal audit is involved in assisting in the internal investigation, that they do so at the direction of, and report to, general counsel or external counsel," says Sloane.

Increasingly, when companies settle a probe, they're tasked with conducting their own reports assessing the compliance program. "If a company has its own self-assessment and reporting requirements, that's going to put additional responsibility on internal audit to prepare those reports," says Sloane, particularly since "one of the things regulators look for are any reports that were issued by the internal audit group on the problem area." ■

ROLE OF INTERNAL AUDIT IN FCPA CASES

Below are examples of FCPA cases where the Justice Department and the SEC have cited alleged internal audit failures and successes.

Examples of FCPA cases where the Justice Department and SEC have cited internal audit failures:

- *SEC v. Biomet* (2012): Biomet's compliance and internal audit functions failed to stop improper payments paid to doctors in Argentina, even after learning about the illegal practices. "Executives and internal auditors at Biomet's Indiana headquarters were aware of the payments as early as 2000, but failed to stop it."
- *SEC v. Oracle* (2012): Oracle "failed to audit and compare" distributor margins against end user prices to "ensure excess margins were not being built into the pricing structure." In addition, Oracle "failed to seek transparency in or audit third-party payments made by distributors on Oracle India's behalf."
- *SEC v. Eli Lilly* (2012): Eli Lilly's audit department had "no procedures specifically designed to assess the FCPA or bribery risks of sales and purchases."

Examples of FCPA cases where the Justice Department and SEC have credited internal audit:

- *U.S. v. BizJet* (2012): "following discovery of the FCPA violations during the course of an internal audit of the implementation of enhanced compliance related to third-party consultants ..."
- *SEC v. Pride International* (2010): "during a routine audit, Pride International discovered an allegation of bribery ..."
- *SEC v. Statoil* (2006): "Statoil's internal audit department reported to Statoil's [CFO] that Statoil had paid $5.2 million under a consulting agreement to an entity that had not been named in the contract ..."
- *SEC v. Chiquita Brands* (2001): "Chiquita's internal audit staff discovered the payment during an audit review ..."

Sources: SEC; Justice Department.

Fighting Fraud and Corruption Is an Inside Job

By Tom Fox (TomFoxLaw), Jimmy Lin (The Network), and Glenn Pomerantz (BDO Consulting)

Let's face it: Fraud, corruption, and bribery are viable threats to all organizations, no matter how ethical they may be perceived. All it takes is one bad actor or one sketchy deal outside the normal borders of operation to put a company's name in the headlines. Compliance programs, geared to address these specific issues, are essential to reduce occurrences in the first place and to limit exposure and liability. Corporate success and risk are uncomfortable but necessary bedfellows; however, organizations can find themselves taking risks every day that stretch their compliance values and slide toward bribery and corruption.

The best compliance programs—and the ones garnering the most accolades—are those that work to address the risks head-on, instead of attempting to play catch-up. When incidents occur, when transaction monitoring, audits, or employee hotlines turn up something amiss, these programs catch them early and deal with them effectively. Regulators like to see that, and it may keep you from getting into hot water.

So what is the view from ground level? What characteristics of a compliance program are effective? And when bribery, corruption, or fraud is suspected, how do you properly investigate the matter so that remedial action can be taken?

First, let us look at some statistics.

According to the SEC's "2013 Annual Report to Congress on the Dodd-Frank Whistleblower Program," more than 3,200 tips were received and processed (an eight percent increase over 2012), and, according to SEC Associate Director of Enforcement Stephen L. Cohen, a "significant majority" of those tips were first reported internally. October 2013 saw the largest SEC whistleblower payout to date—a $14 million award involving investment fraud.

Fraud and corruption contributed to almost one-quarter of incidents reported through employer hotlines, according to The Network's "2013 Corporate Governance and Compliance Hotline Benchmarking Report," analyzed by BDO Consulting. The Network's report also tracks the Corporate Fraud Index, which measures the percentage of reported fraud-related incidents. For the 2012 reporting year, the Fraud Index rose to 23.6 percent, an all-time high since the Index was first reported in 2005.

The advent of the SEC whistleblower bounty program does not seem to have made a significant difference in use by employees of their employers' internal hotline systems as their first point of action in reporting misconduct. Two factors that may be contributing to the continued use of internal employee hotlines include:

1. The SEC whistleblower program provides additional incentives should a whistleblower first report wrongdoing through the company's whistleblower/compliance system, allowing a 120-day period for the organization to self-investigate the claims while protecting the whistleblower's "place in line" for a potential bounty.

2. The inherent delay between the initial notification to the SEC and the announcement of an award may be limiting the potential impact the SEC whistleblower program has on internal reporting mechanisms. Since only six awards have been made to date, potential whistleblowers may not be aware of the financial windfall possible when reporting via the SEC whistleblower program.

Interestingly, The Network's report found that the percentage of fraud and corruption hotline tips that had been previously communicated to management was less than 30 percent. Hence, more than 7 out of 10 of the reported instances of fraud and corruption were either ignored or not acted upon in a satisfactory manner in the eyes of the whistleblower. This phenomenon represents an opportunity for improvement in the compliance function.

Although it may be difficult to comprehend, some organizations may still be inadequately addressing credible hotline tips and/or some are simply papering the file in an effort to avert penalties, fines, and possible criminal sanctions. While most well-intentioned organizations work hard to make their employees aware of internal reporting methods and instill confidence in the confidentiality of the reporting (as well as protections against retaliation), others talk a good game but continue to come up short. In addition, retaliation against whistleblowers is still a major concern, despite SOX and Dodd-Frank protections, and it affects anti-corruption efforts because potential whistleblowers worry about the potential repercussions of their actions. The SEC has stated that it stands ready to investigate any reports of organizations punishing employees for cooperating with the SEC or pressuring employees to forfeit any potential "bounties or awards," both of which are violations of SEC rules.

As a rule, employees want to report internally because of various factors, such as their loyalty to the company, their innate aversion to dealing with regulators, and for their own self-protection (if the company fails, they may lose their job). Employees are, by far, a company's best source of information about what is really going on, and organizations must listen to their own employees, particularly to

help improve processes and procedures. Internal reporting gives organizations an opportunity to understand the problems and take steps to correct these issues, protect their reoccurrence, and prevent potential loss and reputational damage. Again, a company must make it clear that fraud and corruption are taken seriously and that the eyes, ears, and voice of its employees are crucial to efforts to reduce risks.

So, what are the best practices that every organization should follow to fight corruption on a global scale? Taken as principles for a more ethical, corruption-free business, these practices include leadership, policies, training, a fail-safe internal reporting system, transaction monitoring, an engaged workforce, and thorough action in terms of investigation, remediation, and prevention. You should design your program to encourage and reward those employees who take these risks seriously and are in a position to help you in the fight against fraud and corruption. Implement a compliance program that engages your greatest resource – your own employees. Doing this requires the following steps:

Walk the Talk: Leaders must establish and communicate a committed attitude that corrupt practices will not be tolerated at any level of the organization. A successful anti-corruption program must be built on a solid foundation of ethics that are fully and openly endorsed by senior management; otherwise, the program may amount to little more than a hollow set of internal rules and regulations. There should be an unambiguous, visible, and active commitment to anti-corruption. But even more than support or the right tone-from-the-top, anti-corruption standards require that companies have high-ranking chief compliance officers who have the authority and resources to manage the program on a day-to-day basis. Those compliance officers must have the ear of those ultimately responsible for corporate conduct, including the board of directors.

Establish a Solid Code of Ethics: Leverage your Code to directly address the risk of fraud and corruption and set the standards of expected behavior for employees, providing them the guidance they need to act with integrity. Every organization should have a values-based Code of Ethics that expresses its ethical principles. Moreover, your Code of Ethics should be a mechanism to which employees, who are trying to do the right thing regarding compliance, can go to for support and guidance. It is the cornerstone of your compliance program.

Implement Anti-Corruption Policies: Establish strong, specific policies, and drive awareness about these policies throughout the workforce. Every organization should have standards in place that build upon the foundation of the Code of Ethics and articulate code-based policies, which should cover such issues as bribery, corruption, and accounting practices. An organization should then ensure that enabling procedures are in place to confirm those policies are implemented, followed, and enforced.

Foreign Corrupt Practices Act (FCPA) compliance best practices suggest that organizations have additional standards and controls, including, for example, detailed due diligence protocols for screening third-party business partners for prior criminal acts, financial stability, and associations with government officials. Ultimately, the purpose of establishing effective standards and controls and promoting them throughout the organization is to demonstrate that your compliance program is more than just words on paper.

Train and Communicate to Your Employees: Another pillar of a strong anti-corruption compliance program is the proper training of company officers, employees, and third parties on relevant laws, regulations, corporate policies, and prohibited conduct. Simply conducting training usually is not enough. Enforcement officials want to be certain the messages in the training actually get through to employees. Expectations for effectiveness, per SEC/DOJ guidance, are measured by whom the company trains, how the training is conducted, and how often it occurs. But training alone isn't enough. It's essential to maintain ongoing communications regarding corruption, up and down the chain, which means that resources (possibly including a "triage" committee) must be dedicated to providing answers to situational questions as they arise.

Establish a Speak-Up Culture and a Confidential Internal Reporting System: In so many ways, your own employees are your best source of information. You should encourage internal reporting by making them aware of all reporting mechanisms as well as the priority the company places on having a corruption-free culture. Create open-door policies to facilitate face-to-face meetings. Work to provide phone- and Web-based anonymous reporting and drive confidence in your reporting programs via follow-up communications and proper escalation procedures. Implement policies and procedures to prevent retaliation and make it clear that you will have no tolerance for negative actions against those employees who, in good faith, report compliance concerns.

Implement Oversight, Including Monitoring and Auditing: How do you know if your employees have taken

your compliance message to heart? Even after all the important ethical messages from management have been communicated to the appropriate audiences and key standards and controls are in place, a company should still be vigilant in determining whether its employees are following its compliance program. Many companies fall short on effective monitoring. In part, monitoring is a commitment to reviewing and detecting compliance program anomalies in real time and then reacting quickly to remediate them. A primary goal of monitoring is to identify and address gaps in your program on a regular and consistent basis.

Listen to Your Employees: You should always take the opportunity to listen to what your employees have to say about corruption risks. You should proactively assess your risks through employee surveys to help uncover and detect possible corruption or fraud before it becomes a larger issue, if not before it even occurs. Listening also ties in directly with your training. It is important that you pay attention to what employees say during these sessions, because training can alert you to potential problems based on the type of questions employees ask and their level of receptiveness to certain concepts. For example, during training employees might ask specific questions about important compliance considerations, such as their interactions with government officials or gift-giving practices. Such questions can raise concerns and uncover issues that should be reviewed and addressed quickly. In-person training along with methods for disclosure during online training are particularly useful in this regard, especially for higher-risk employees such as those involved in sales, business development, finance, and accounting.

Take Insightful Action: After you detect fraudulent or corrupt behavior, prevention of future occurrence is essential. This occurs through remediation. A key concept behind the oversight element of compliance is that if companies are policing themselves on compliance-related issues, the government may be less likely to perceive the need to do it for them. Remediation, then, is an important component of oversight. In the end, it is not enough to just gather information and identify compliance problems through monitoring and auditing. To fulfill this essential element of compliance, you also have to respond and fix the problems.

Fraud and corruption may still be significant risks at organizations with a robust anti-fraud compliance program that has been properly designed, implemented, and monitored. How is this possible?

First, an anti-corruption program can fail to prevent bad behavior but still be considered effective if it detects fraud at an early stage. Earlier detection is a hallmark of an effective anti-fraud compliance program. Preventing fraud that results from a rogue employee or collusion between an employee and a vendor may be quite difficult under most circumstances. However, early detection can limit the impact such frauds have on the organization.

Second, the lessons an organization and its employees learn from experiencing fraud can prove invaluable in the future. Many organizations that, at one time, had implemented adequate anti-corruption compliance controls require a "wake-up call." Although an organization in this category may have designed an anti-corruption compliance program several years ago, the program may not have kept pace with the changing business environment or changes to the organization's business model. Despite the cost and distraction of a thorough fraud investigation, there are substantial long-term benefits when a fraud investigation is conducted in a manner that yields comprehensive recommendations for control enhancements and best practices.

Fraud, bribery, and corruption investigations are rarely simple and usually do not follow a script. The objective of these investigations from the forensic accounting perspective is to determine the facts and circumstances of the transgressions, including who knew what and when, potential additional exposures, control deficiencies, necessary remediation, and mitigation. The following discussion, neatly categorized as the "P" factors, may provide insights into the forensic accounting investigative process and potential pitfalls.

1. The Players: Fraud cannot happen without people, so you must take into account all the various "people factors" that are involved, including the cultural differences among global employees, the various departments, and disciplines in which those employees are involved and the interests of each. For example, risk assessments should include an analysis of what pressures and motivating forces drive employees and third parties to act outside the bounds of expected behavior. Investigations include similar assessments. Questions a forensic investigator should endeavor to answer in an investigation include, "Who has behaved in a manner inconsistent with my expectations? Who appears to exceed their authority? Is that behavior an indicator of an accomplice?"

2. Pressures: Time is almost always of the essence in a fraud investigation. When an incident occurs, it seems that public reporting deadlines are never more than a few weeks away, disclosure requirements are due al-

most immediately, and senior management and all other interested parties are demanding immediate answers—often under complex circumstances. A commitment to determining the facts must take priority over filing deadlines. A special committee or board that instructs its professionals to act otherwise should be viewed with skepticism.

3. Preservation & Privacy: Perhaps the most overlooked aspect of corruption investigations are the critical steps that should be taken at the outset of the investigation, most notably a preservation order and protection of all potentially relevant electronic and hard-copy evidence, all within the confines of privacy laws in multiple venues. Preservation orders may be delicate as they often let the proverbial cat out of the bag. Employees, business partners, and stakeholders may grow concerned and, at worst, panic. Meaningful communications from the company's leadership may assuage such feelings and lead to cooperation with investigators. Privacy laws must be addressed early and thoroughly by qualified counsel with experience in the relevant jurisdiction. Inadvertently reviewing an employee's private e-mail, despite it residing on the company's server, could be a criminal offense in several countries.

4. Performance: The proficiency of the investigative team is often taken for granted, but designing an effective team is best approached well before an allegation surfaces. Investigative planning can lead to superior investigative performance, including team members who work well together and know their roles. Planning is an integral part of a proper fraud investigation process, so the ability to have boots on the ground in a timely manner is important for quick resolution. Investigation teams are also potentially faced with overcoming cultural and language barriers and local legal constraints. Performance measures of the investigation team include how well they prioritize responsibilities and issue assignments to its most qualified team members.

5. Publicize: The question of whether to self-report and what to publicize is a decision made collectively by senior leadership, usually the board and its advisors in the case of a larger corporation. Self-reporting has been a widely discussed issue, but concerns like whether to disseminate investigative results to the whistleblower or to other employees can be overlooked as can the importance of timely remediation when controls were lacking or over-ridden.

Looking at the global business climate with a pessimistic eye, it may seem that fraud and corruption are inevitable, or even an expected consequence of human nature. Industry benchmarking reports indicate that fraud reporting is still on the rise, and the SEC whistleblower program is receiving more and more tips and encouraging more reporting by stepping up rewards to whistleblowers. There is also renewed attention to global anti-bribery as illustrated by newly enacted laws in Russia, China, Brazil, and Italy among other countries, as well as a continued prosecutorial focus in the United States.

With a more optimistic eye, an ethical enterprise that is addressing corruption risks merits our respect and even our patronage. We can grasp the advantages of how doing business with integrity and compliance can improve the performance of our organization. It's in the "how," not just the "why," that anti-fraud programs are effective at protecting the enterprise as a whole.

At the organizational level, much can be said for internal control measures and compliance-focused processes, including risk assessments, monitoring, internal reporting, proper investigative practices, and remedial action. Still more can be said for a values-based approach, where senior leaders promote both the intrinsic and extrinsic benefits of an ethical culture throughout the organization, supported by understandable policies, training, and awareness that encourage employees to engage in the compliance process. ■

About BDO Global Forensics

Serving multinational clients through a global network of more than 1,200 offices in 144 countries, BDO's global forensics professionals assist organizations and their counsel to address cross-border and complex matters involving the risks associated with fraud and corruption, as well as a range of litigation and dispute advisory services.

About The Network

The Network is the leader in integrated governance, risk and compliance (GRC) solutions that help organizations mitigate risk, achieve compliance and ultimately, create better, more ethical workplaces. We help thousands of global organizations in every industry, representing nearly half of the Fortune 500 and almost 27 million employees worldwide.

About the Authors

Tom Fox is an FCPA Compliance and Risk Management Attorney and Consultant and Principal at tomfoxlaw.com (tfox@tfoxlaw.com). Jimmy Lin is the VP of Product Management & Corporate Development at The Network, a leading provider of integrated GRC solutions (jimmylin@tnwinc.com). Glenn Pomerantz is a Partner at the professional services firm of BDO Consulting (GPomerantz@bdo.com).

More Cops on the Global Anti-Corruption Beat

By Jaclyn Jaeger

During the last several years, the United States has pursued global corporate bribery and corruption cases with vigor. Now many other countries are getting into the act, with new corruption laws and added enforcement muscle.

According to a report by TRACE International, an anti-bribery group, 15 countries initiated their first-ever bribery enforcement action last year, including Guinea, Kenya, Iraq, the Philippines, and Tunisia—solid proof that more cops are on the global anti-corruption beat than ever before.

Other anti-bribery organizations are also noticing a rise in anti-corruption enforcement on a global scale. Since the Organization for Economic Co-operation and Development convened its Convention on Combating Bribery of Foreign Public Officials in International Business Transactions in 1999, 14 of the 40 countries that have joined the Convention have sanctioned 221 individuals and 90 entities for foreign bribery, according to new anti-bribery data released in June by the OECD.

According to the TRACE report, 25 countries and two public international organizations—the United Nations and the World Bank—have pursued 468 foreign bribery enforcement actions since 1977, when the United States passed the Foreign Corrupt Practices Act and first made such bribery illegal. Additionally, 64 countries have pursued enforcement of domestic bribery laws, with considerable overlap in the countries that have pursued enforcement of both.

To some critics, this figure is still far too low, but enforcement actions continue to rise and more countries are feeling pressure, "so that they continue to increase their anti-bribery enforcement," says Patrick Moulette, head of the anti-corruption division of the OECD.

The United States holds the strongest enforcement record, with 2.5 times as many enforcement actions as all other countries combined since 2002. Specifically, the Department of Justice and the Securities and Exchange Commission pursued 302 foreign bribery enforcement actions (65 percent of all foreign bribery cases). This figure includes eight times as many actions as the United Kingdom, which brought the second highest number of cases, with 38 enforcement actions.

"The level of attention and degree of priority given to fighting bribery varies widely, depending on the risks relative to each country's economy," notes Moulette. For example, how involved is the country in the extractive industry? Is the country a major economy with strong export sectors? Does the country have a lot of foreign investments? "Those are important factors to keep in mind when we look at enforcement carried out in each country," he says.

In the United States, for example, many of the enforcement actions brought by the Justice Department and SEC focus on companies and individuals that violate the FCPA by paying bribes to foreign government officials. By comparison, other countries—such as South Korea, Nigeria, and China—place particular emphasis on prosecuting corruption within their own governments.

> "The harsh penalties associated with the Bribery Act have greatly increased the incentives for corporates to self-report, rather than risk being caught out by a hostile SFO investigation."
>
> Barry Vitou, Partner, Pinsent Masons

U.S. enforcement agencies are not only pursuing U.S. companies for FCPA violations. For companies that face formal charges by the Justice Department or the SEC or are the subject of ongoing investigations, 25 percent involved companies headquartered outside the United States. Most were headquartered in the United Kingdom, the Netherlands, and Germany, followed by Switzerland and Japan.

The TRACE report also found that, when it comes to enforcement actions for "inbound" bribery—bribes that a country's government officials take from foreign companies—South Korea and Nigeria lead the world in enforcing their national prohibitions. South Korea recorded 17 of the 164 total inbound global enforcements recorded, while Nigeria had 15, followed by China with 11.

How successful a country will be at enforcing bribery and corruption is "a question not only of budget and number of staff," Moulette says, "it's a question of specialized expertise."

Because many of these bribery cases are labor-intensive and often involve a high-level of forensic accounting, the more cases a country takes on, the more adept it becomes at handling such matters, says Alexandra Wrage, president of TRACE.

She cites the aftermath of the Siemens case as an example. "It's no coincidence after the Siemens case that Germany brought a whole series of other cases in rapid succession," Wrage says. "They already had a sophisticated legal system,

but now they have prosecutorial experience with pursuing a bribery case."

More Fessing Up

For the first time this year, the report also included data on how many times countries declined to take formal enforcement actions or closed official inquiries related to bribery. With 22 declinations since 1977, the United States showed the highest number by a significant margin.

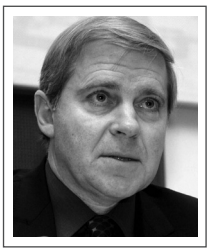
Six other countries also declined to pursue formal bribery enforcement actions in that period. The United Kingdom had the second highest number with three declinations, while South Africa, Russia, Norway, New Zealand, and Khazakstan all had one declination.

Wrage says the number of declinations observed by the report is not surprising. A company has to self-disclose to get a declination. "The United States certainly, without any question at all, has the highest level of voluntary disclosures," she says.

The number of U.K. companies to voluntary self-disclose potential wrongdoing to the Serious Fraud Office continues to rise, nearly doubling in the last fiscal year, according to analysis conducted by law firm Pinsent Masons. Twelve companies have self-reported white-collar crime to the SFO in the year ending March 31, compared with just seven during the two preceding years.

"The Bribery Act is already having a big impact on corporate attitudes toward rooting out and self-reporting white-collar crime," Barry Vitou, a partner at Pinsent Masons, stated in a client alert. "The harsh penalties associated with the Bribery Act have greatly increased the incentives for corporates to self-report, rather than risk being caught out by a hostile SFO investigation."

Wrage says more companies would be willing to self-disclose if they knew the odds of receiving a declination. Historically, information pertaining to declinations has been "shrouded in secrecy," and even now is difficult to come by unless companies make their declinations public, she says.


Moulette

While enforcement has increased overall, much more work needs to be done. For one, the OECD is still missing a few major economies, including China, India, and Indonesia, says Moulette. And still other countries have yet to bring a single conviction, prosecution, or investigation, he says.

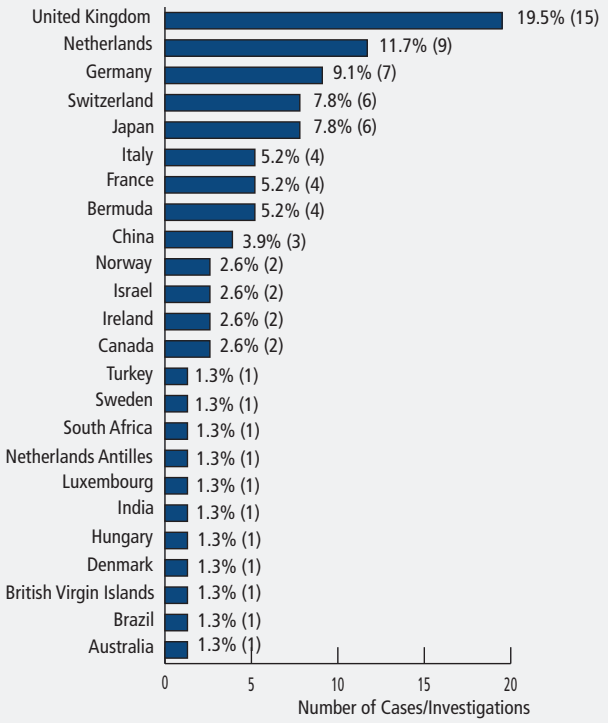
It's true, too, that the actual number of global enforcement actions actually declined last year. The United States experienced the sharpest decline, dropping from 42 enforcement actions in 2011 to 20 last year (excluding ongoing investigations). In comparison, all other countries' foreign bribery enforcement actions declined by 42 percent, from 12 in 2011 to seven last year.

Although the numbers are down, anti-corruption trackers say that is likely a temporary lull, rather than a developing trend. "Based on what we hear about cases in the pipeline and based on we're seeing about growing international interest in enforcement," Wrage says, "everyone should assume the trend is going to continue up."

Many anti-bribery cases in the pipeline take a long time to resolve and have a way of skewing enforcement numbers, Wrage says. Looking at the overall picture, the real message is that "anti-bribery enforcement is here to stay and trending upward," she says. ■

FOREIGN BRIBERY ENFORCEMENT ACTIVITY

The following chart details the United States' enforcement of foreign entities from 1977 through 2012.



Source: TRACE.

Anti-Corruption Policies: What Regulators Want

By Amy Burroughs

Don't expect the crackdown on international corruption by U.S. regulators to ease up anytime soon.

Speaking at the Compliance Week 2013 conference in Washington, D.C., representatives of the Department of Justice and the Securities and Exchange Commission said the agencies expect that when red flags for potential violations of the Foreign Corrupt Practices Act arise, companies will react quickly to investigate.

Charles Duross, deputy chief of the Justice Department's FCPA Unit, and Kara Novaco Brockmeyer, chief of the SEC's FCPA Unit, said investigators do not expect a pristine environment, but they expect companies to have a program in place to combat corruption and that they follow it. Paul McNulty, a partner at law firm Baker & McKenzie and former U.S. deputy attorney general, moderated the discussion.

Recognition is growing that "good on paper" is not good enough, Brockmeyer said. "You have to kick the tires and see 'does it really work in practice?'"

Brockmeyer also pointed out that although anti-corruption programs are more sophisticated, there are still plenty of indications that corruption and fraud are widespread at many companies. For example, the findings of Ernst & Young's *2013 Europe, Middle East, India, and Africa Fraud Survey*, released May 7, indicate that companies still have a lot of work to do. The survey found that one in five employees is aware of financial manipulation in their companies, and 42 percent of senior managers and board directors know of irregular financial reporting. "I would be extremely concerned about some of the data that came out of that report," Brockmeyer said.

To combat those concerns, and to give companies a better sense of the regulators' expectations, she and Duross explained their views of what a robust compliance program should look like. Both worked on guidance issued last November in the publication, "A Resource Guide to the U.S. Foreign Corrupt Practices Act," to provide more detail on FCPA enforcement.

"My message is that FCPA compliance and FCPA issues aren't limited to one industry or one country or any particular size company or whether it's a U.S.-company or foreign-based company," Duross said. "It covers the gamut."

He described as naïve managers who believe they can land business with a bribe and then keep the contract through stellar products and service. In reality, he said, they are entering a vicious cycle: "The first bribe is exactly that—the first bribe in a series of bribes."

Measures of Success

One of the best signs of a successful program, according to Brockmeyer, is that concerns rise to the surface.

Pictured above: Paul McNulty (left), former U.S. deputy attorney general; Kara Brockmeyer, chief of the SEC's FCPA unit; and Charles Duross, deputy chief of the Justice Department's FCPA unit.

She said that an environment where employees aren't raising concerns doesn't mean that no problems exist. "If your compliance program is telling you 'We don't have any problems,' maybe that is one red flag you want to take a look at," she said.

Duross emphasized that how a company responds to red flags has significant bearing on any investigation. If an audit or a hotline report prompts compliance staff to look into an issue, they may determine no problem exists. What matters to the government is that a program was in place and it was followed. "The fact that procedures and processes worked to achieve an ultimate resolution shows that this is not just a paper program," Duross said.

Companies score points—"meaningful credit," in FCPA parlance—when they can tell investigators exactly what they did in response to a concern.

So what, exactly, is Duross hoping to hear? When a compliance officer says in response to a question: "I was wondering the same thing and let me tell you what we did." That demonstrates a good-faith effort to get it right and carries tremendous weight with investigators, he said.

Duross also pays attention to a company's discipline history, and is skeptical of those that don't have one. "You have how many thousands of employees and you operate in how many companies and you're telling me no one has been disciplined in the last five years? That tells me either you have a perfect company…or you have such profound problems you're not dealing with any of it."

Consistency and an even-handed approach are also good signs. If a low-level employee is fired for the same behavior a sales director skates on, said Duross, that sends the wrong message: Different standards apply to money-makers.

Trouble Spotting

Two of the trouble spots that the regulators urged companies to focus on are acquisitions and third parties. More vetting of third parties provides an opportunity to re-assess those relationships, and companies may even find that corruption risks are too great to do business with some third parties. One CEO told Duross, for example, that compliance efforts led him to reconsider the business model of spending so much on third parties, some of which added little value.

Brockmeyer said that companies should be careful with acquisitions where they find other problems, since that could be an indication that corruption is lurking under the surface. "At some point, one red flag may turn into two or three, and you may need to revisit," she said.

She also said that buying a company, especially in regions where bribery and kick-backs are sometimes considered part of doing business, is a risky proposition. "If you get in and find their business model is based on corruption, you're also likely to find they're not complying with the same good accounting principles we use in the United States," she said.

A company may spot a red flag, but be unable to dig into the matter until the relationship progresses. Investigators know red flags crop up, Brockmeyer said, but what matters is a company's reaction. It's the difference, she said, between engaging in a third-party relationship for a few months and then calling it quits when concerns are confirmed, versus ignoring concerns for years.

At the Justice Department, Duross said, investigators want to see evidence of solid due diligence on vetting acquisitions and third parties. Thin or empty files on third parties put them on alert.

The SEC is noticing more cases of third-party distributors that provide a legitimate service, but have an "extra" service on the side. Compliance officers should ask hard questions about what exactly distributors are doing to earn that extra commission, Brockmeyer said.

She also clarified the SEC's stance on successor liability, saying an overseas subsidiary becomes subject to the FCPA at the time of acquisition. "If you look at … successor liability cases, really what they're getting hit for is they didn't catch problems after the acquisition," she said. "We're talking years, not months."

In cases where companies come forward some months later to report they found—and fixed—a problem, the SEC generally declines, she said.

Deferred Prosecution Agreements

Between declinations and prosecutions lie deferred-prosecution agreements (DPAs), which allow companies to meet obligations under Justice Department oversight—"trust but verify," Duross explained.

DPAs should not be confused with the idea that regulators are going easy on companies that agree to them, said Duross. "Anybody who has gone through a deferred prosecution agreement with us will know we ask tough questions and we continue to," he said. But, they do give the Justice Department leeway to determine individual outcomes. "It's been my experience, anecdotally, companies see these as an opportunity to turn themselves around in a meaningful way," he said.

Equally important, such agreements reward companies that report wrongdoing, while holding them accountable. From the Justice Department's perspective, that may compel others to follow suit. "I recognize companies have a very serious decision to make when it comes to voluntary disclosure," Duross said. "[DPAs] can be a powerful tool to do the right thing."

At the SEC, DPAs and non-prosecution agreements are a newer tool. The SEC's first FCPA-related NPA, in fact, was announced in April: Ralph Lauren Corp. will surrender more than $700,000 in illicit profits it obtained through a subsidiary's bribes to Argentinian officials. Under a separate NPA with the Justice Department, Ralph Lauren Corp. will pay a penalty of $882,000 and agree to improve its compliance program.

In a press release issued at the time, Brockmeyer said the NPA was based on Ralph Lauren's self-reporting, cooperation, and discovery of the bribe through an enhanced compliance program. "Even if you have identified a problem and you don't have a good explanation … there are a lot of steps you can take at that point to improve the resolution going forward," she said. ■

THINGS OF VALUE

Below are examples of improper travel and entertainment:

- A $12,000 birthday trip for a government decision maker from Mexico that included visits to wineries and dinners
- $10,000 spent on dinners, drinks, and entertainment for a government official
- A trip to Italy for eight Iraqi government officials that consisted primarily of sightseeing and included $1,000 in "pocket money" for each official
- A trip to Paris for a government official and his wife that consisted primarily of touring activities via a chauffeur-driven vehicle

Sources: Justice Department; SEC.

Create a Better Workplace.

Fraud and corruption rob global organizations of time, revenue, reputation and even their greatest asset — their people. An effective compliance program is your best line of defense against liability and proves that your organization values ethical business and will not tolerate corruption.

- **Protect** your employees, your reputation and your bottom line, with confidence and security.
- **Detect** and prevent ethics and compliance issues using a comprehensive, collaborative approach.
- **Correct** risk issues across the enterprise and connect compliance with performance.

Gain valuable insight into your ethics and compliance initiatives, across your entire enterprise, with the Integrated GRC Suite from The Network.

grc 20/20 Technology Innovator 2013

www.tnwinc.com | 1.800.253.0453

THE Network
Integrated GRC Solutions