COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2023

Mark Jenkins (mjenkins@kreller.com) is the Director of Forensic Investigations with the Kreller Group in Dallas, Texas, USA.

"GOAT" compliance programs

By Mark Jenkins, CFE

I have always loved to compete in sports, even though I have been consistently mediocre. In contrast, I like to watch sports because I like watching the Greatest Of All Time—a.k.a. the "GOAT."

People will always debate about the GOAT in each sport. Tom Brady, with seven Super Bowl victories, is a great candidate for football. Serena Williams has won 23 major singles titles, dominating women's tennis for the last two decades. My personal all-time favorite is Earvin "Magic" Johnson, who won five NBA titles in basketball in the 1980s. Each checked many boxes: they had great technique and intangibles, worked to improve aspects of their craft in the off-season, and had solid overall game IQ. All have at least one thing in common: results. They won—a lot—at the highest levels of their respective sports.

What about the gold standard in anti-bribery/anti-corruption (ABAC) compliance programs? What makes a program the GOAT? Whatever the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) demand of companies? The DOJ/SEC guidance in the last decade should be part of every compliance program because, as we will explore, it sets a standard. However, continuous monitoring—which includes regularly conducting third-party audits—is also necessary for GOAT status and, more importantly, to detect and prevent corrupt activity.

What are the regulatory demands?

The DOJ/SEC, for the last decade, has supplied several guidance documents, including *A Resource Guide to the U.S. Foreign Corrupt Practices Act* which details what it expects in corporations' ABAC compliance programs. They expect that a compliance program is well-designed, in good faith, and uses continuous monitoring. They also set forth the following statement:

> "Third, companies should undertake some form of ongoing monitoring of third-party relationships. Where appropriate, this may include updating due diligence periodically, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party."[1]

Compliance officers might push back and claim, "Well, this is just guidance."

However, take this random selection of DOJ enforcement actions against 20 companies from the DOJ website in the last five years (2017–2022)—there is no statistical significance in my selection—and review specific points from indictments, information documents, and DOJ press releases (see Figure 1).[2]

Figure 1: 20 Enforcement actions

Description	No.	%
Failure to Disclose	20	100%
Third-Party Intermediary	17	85%
Companies Monitored	13	65%
Received Credit	8	40%
Disguised Payments	8	40%
FCPA Repeat Offenders	5	25%
Total Reviewed	**20**	

None of the 20 companies (I did not look at individuals charged) voluntarily disclosed their bribery issues. There could be many reasons the 20 did not: counsel may have recommended that they not reveal, the entity did not believe they would be discovered, the compliance program did not include continuous monitoring, or the compliance program did not catch the issue when it occurred. Regardless, not voluntarily disclosing the bribery issues appears to have cost the offenders in the penalty assessment phase.

Seventeen out of 20 (85%) enforcement actions involve bribes being funneled through a third-party intermediary (TPI). The DOJ assigned 13 entities (65%) a monitor, meaning the DOJ had no confidence that the entity's compliance program was adequately equipped going forward. An entity being assigned a monitor is equivalent to the "death penalty" in NCAA sports. The company must pay the monitor to micro-analyze the development or enhancement of the compliance program over several years. Monitors are usually legal or consulting firms with substantial billable rates.

Five of the randomly chosen companies were repeat offenders. At least three had three or more offenses.

Based on this back-of-the-envelope analysis, TPIs often participate in corrupt activity and, overall, inadequately designed compliance programs by the offenders are evidenced. DOJ shows no signs of slowing down—nor are the trends deviating from assigning costly monitorships. Compliance officers should take heed to ensure their program's integrity and focus on the highest risks.

Risk scoring TPIs

Despite the above findings on third-party involvement in corruption, companies realistically need to conduct a cost/benefit analysis, as most organizations need help to afford to conduct due diligence and/or TPI audits on every vendor.

Before deciding if a TPI should be audited, a risk-scoring exercise is warranted. Entities can go through varying levels of sophistication as part of risk scoring. If a company does not risk score its TPIs wisely, costs will not be distributed to the greatest areas of concern. Risk factors and questions to consider can include:

- The geographic location of the TPI and where it conducts business determine prominent levels of

corruption in those countries.

- Identifying TPIs with contact points with foreign government officials and where those contact points are in the transactions (e.g., customs, taxes, licenses, permits such as building a facility, and visas).
- The revenue generated through the TPI.
- The role of the TPI. Is the intermediary a commercial agent, broker-dealer, distributor, professional services provider, or selling products directly to the company?
- History with the TPI. Has the company conducted business with the TPI in the past, and if not, how was the TPI introduced to the company? Did a foreign government recommend the TPI? Did the TPI approach the company?
- The reaction by the TPI to a due diligence investigation conducted on the TPI and its owners. Was there pushback when requesting financial or ownership information? Was the due diligence questionnaire filled out completely?
- The results of the due diligence investigation, were there red flags and, if so, what was the nature of the risk concern(s)?[3]

Choosing TPIs

Based on risk scoring, a prioritized list of high-risk vendors should be developed, and audits conducted on the highest-risk TPIs. If red flags were found in the due diligence and the company decides to continue doing business with the TPI, then the company should audit the TPI as soon as possible before going forward.

Audit steps and techniques

Audit team

Before an audit begins, assemble a qualified team. The team should consist of experienced investigators and forensic accountants familiar with obtaining and analyzing large accounting and financial datasets. If the team members are external to the company, the company's internal auditors or compliance professionals should be part of the team since they should understand the company's business operations. Also, it is important to use the local country's resources to familiarize themselves with the local customs, language, regulations, and business processes. You may think that sounds like a lot of people for an audit. Typically, you can find practitioners with many of these skill sets; therefore, fewer people will be needed.

Audit objective

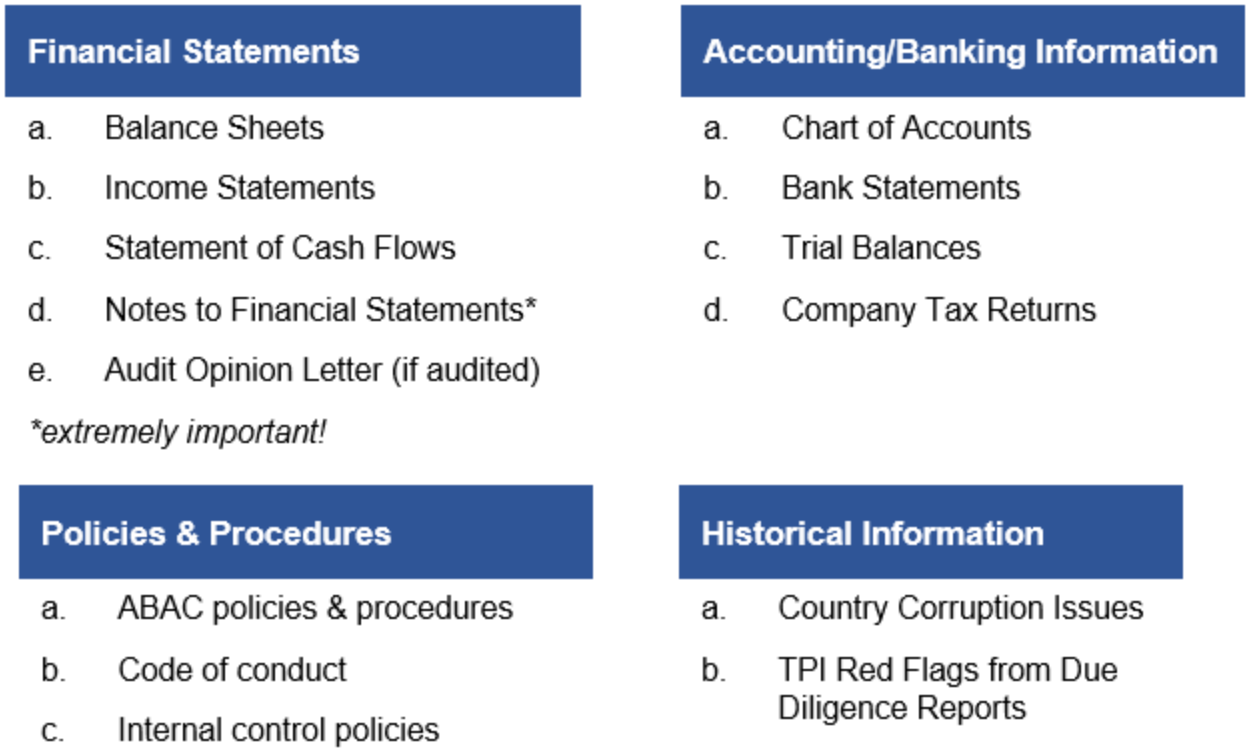
The goal of the audit should be discussed and solidified. Generally, audit goals should be identifying areas of risk in (a) the entity's compliance programs, (b) transactions, and (c) the key owners/employees (tone at the top).

To meet these objectives, discussions with key employees should be conducted to determine their level of understanding concerning ABAC compliance, internal controls, and their attitudes towards both.

Sample document request

Although each TPI's audits are unique, a typical document request (covering at least two years and the most current year) should include several resources (see Figure 2).

Figure 2: Document request examples



Employee interviews

Discussions with TPI key employees/owners will be needed; therefore, use experienced interviewers who understand this is not a deposition nor a forensic interrogation/elicitation interview. Professionals leading the discussion should never be heavy-handed; however, it is critical to maintain "professional skepticism" and probe further if answers do not appear to be fruitful. Professional skepticism means not accepting answers to questions or the documents provided at face value without investigating further. For instance, if TPI representatives say they conduct third-party due diligence investigations on high-risk vendors, you should request and review those reports.

Below is an example of where professional skepticism was warranted, from a case study conducted by Kreller:

> On behalf of a lender, Kreller conducted due diligence on a borrower. Based on interviews with the borrower, it seemed appropriate to review underlying documents. There were significant findings that the third party (of the borrower) had historical fraud issues. In reading the contract (between the borrower and TPI) and payment information, the borrower hired the TPI despite the due diligence red flags and paid the TPI hundreds of thousands of dollars annually to obtain licenses from government entities in a highly corrupt country. Since the lender decided to "dig deeper" and show professional skepticism, the lender was able to make informed decisions. Based on the above and other findings and information, the lender decided to discontinue funding.

Transactional testing

Typically, the audit will start with a review of the policies, procedures, and financial information. The interviews

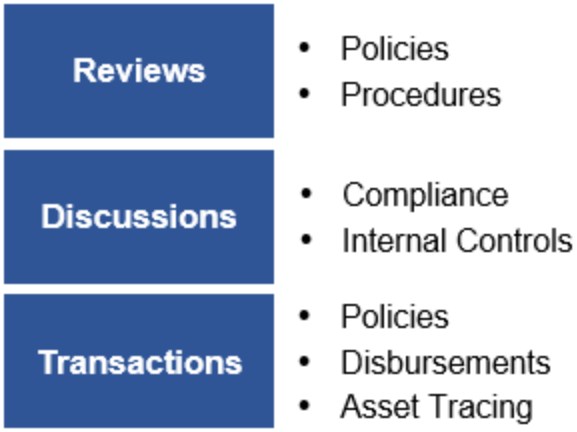
will guide where the focus of the transactions should be. Depending on the services provided by the TPI and its interactions with government officials, tracing the payments made to the TPI from the company and then the TPI to third parties may be a main area of focus. Identifying charts of account descriptions used in bribery payments (or historical frauds specific to the company) should be reviewed, and transactions analyzed. In the 20 companies evaluated in the earlier section, the following terms (and abbreviations) used to pay bribes were found: commissions, commission payments (CP), remuneration, incentive payments (IP), advances, consultant payments, engineering fees, and advance payments (AP). There are many others to review, such as entertainment, gifts, miscellaneous, meals, etc.[4]

If these or similar terms are found, review support for these transactions.

Here are the three steps in the audit process (also summarized in Figure 3):

1. Reviewing what the company says it does (i.e., policies and procedures used to implement and enforce those policies).
2. Talking to employees to understand what the employees say they actually do in accordance with those policies.
3. Testing whether what the company and employees stated (and documented) is consistent and demonstrated within actual transactions.

Figure 3: Three steps of the audit process



Final thoughts

It is essential to integrate your findings and update your compliance program based on results of the risk assessments, internal investigations, and TPI audits (much like the sports GOATs who continually enhance their skills off-season). The ABAC compliance program must become smarter and evolve as new information is incorporated and potential risks uncovered. The regulatory agencies will not tolerate "dusty" ABAC programs created and left on the shelf.

Takeaways

- Compliance programs should incorporate Department of Justice guidance.
- It is essential to audit high-risk third-party intermediaries (TPIs).

- Integrate the results of your audits into your policies.
- Transaction testing should confirm policies and discussions.
- A TPI audit should accurately assess risk and be conducted with professional skepticism.

1 U.S. Department of Justice, Criminal Division, and U.S. Securities and Exchange Commission, Enforcement Division, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, second edition, updated July 2020, 62, https://www.justice.gov/criminal-fraud/file/1292051/download.
2 U.S. Department of Justice, Criminal Division, "Enforcement Actions," website, database, last updated February 14, 2022, https://www.justice.gov/criminal-fraud/enforcement-actions.
3 Jaclyn Jaeger, "Best practices in preventing a third-party data breach," *Compliance Week*, January 7, 2019, https://www.complianceweek.com/third-party-risk/best-practices-in-preventing-a-third-party-data-breach/24704.article.
4 U.S. Department of Justice, Criminal Division, "Enforcement Actions."