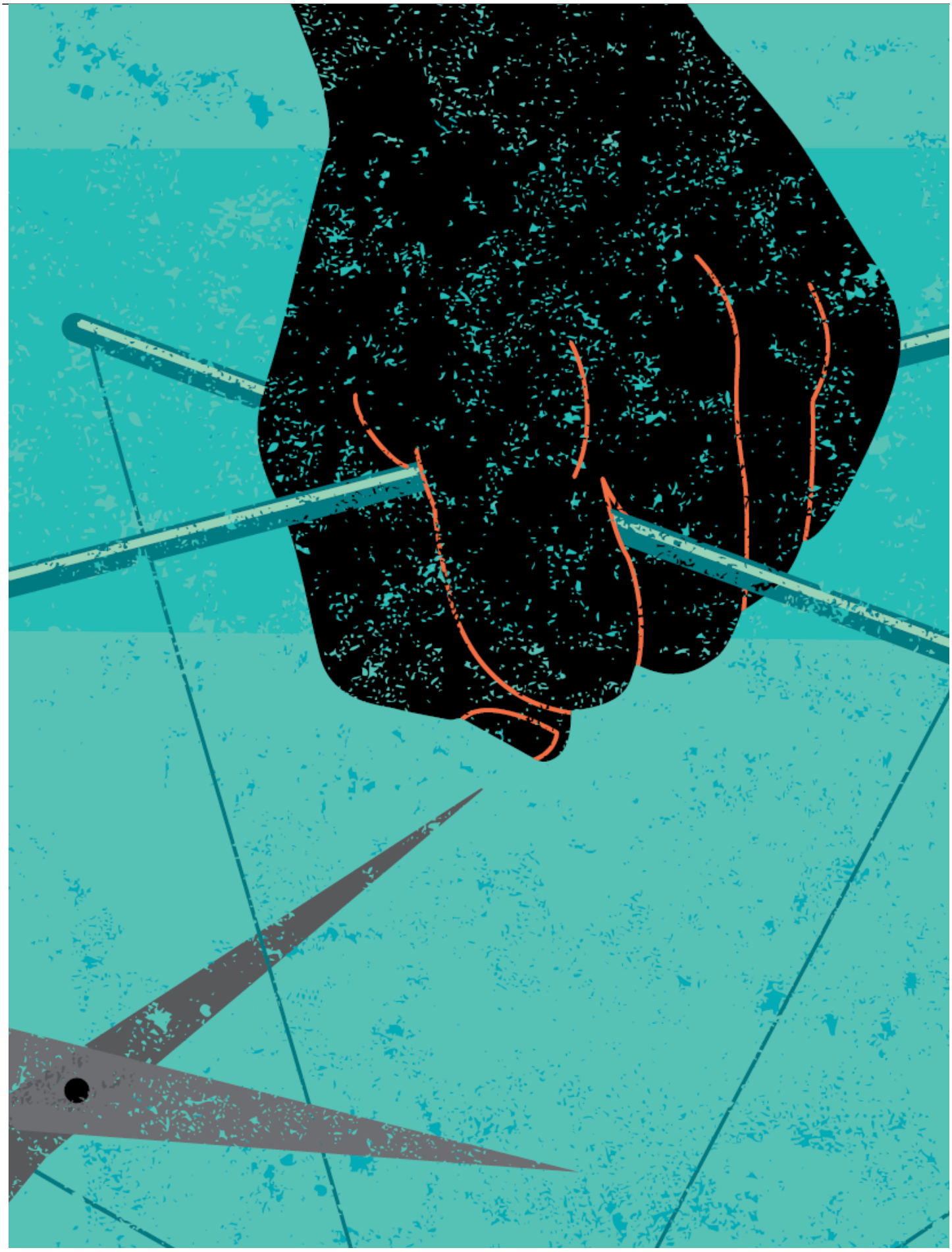
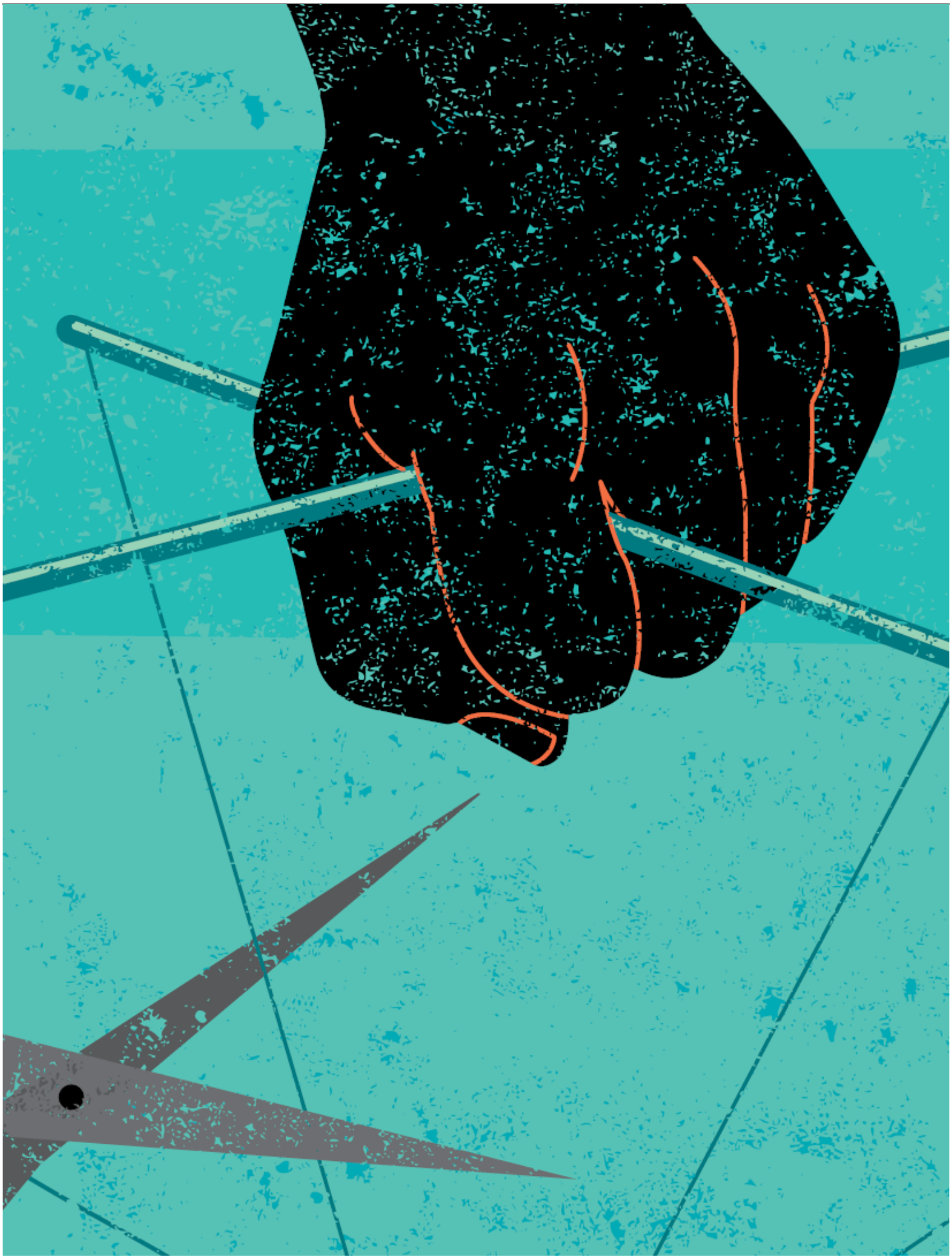
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How-To Manual on Creating and Maintaining an Anti-Corruption Compliance Program

Compliance and Ethics





CHEAT SHEET

- ***Top down.*** The decision must come from senior management, since the culture of compliance starts at the top. Risk assessment then follows, according to the location, the type of operation and a company's third-party partners.
- ***Clarity.*** A code of conduct is the cornerstone of any compliance efforts, and internal anti-corruption policies should address risks associated with business activities including gifts, meals and charitable contributions. Those policies must be communicated to every corner of a company's operations.
- ***Show some teeth.*** Organizations must be willing to remediate and discipline violators at any level, and those penalties should be spelled out and documented when applied. Compliance programs should be regularly reviewed and training supplemented.
- ***Fast response.*** An effective compliance program must respond efficiently to allegations of potential violations. Immediately upon receipt, the allegation should be evaluated, and reported incidents should be documented.

The FCPA prohibits US companies and individuals, as well as issuers, regardless of location, from bribing foreign government officials. More specifically, the anti-bribery provisions of the FCPA prohibit the giving or offering — directly or indirectly — of gifts, payments or "anything of value" to foreign government officials. The FCPA also requires issuers whose securities are listed in the United States to devise and maintain accurate books and records and to make and keep a reasonably effective system of internal accounting controls. The US Department of Justice (DOJ) and US Securities and Exchange Commission (SEC) jointly enforce the FCPA.

Penalties for FCPA noncompliance are severe. The average cost of corporate monetary resolutions is at an all-time high. In 2014, the average total value of monetary resolutions in corporate FCPA enforcement actions was $156,610,000. This is up from $80,070,000 in 2013 and $21,710,000 in 2012. While the corporate monetary resolutions can be large, oftentimes legal and accounting investigative costs exceed the criminal fines. The Avon resolution is an example. In December 2014 Avon Products Inc. settled with the FCPA for $135 million. More staggering, however, is that over a period of five years, Avon reported it spent more than $300 million on "professional and related fees" associated with the FCPA investigation and related compliance reviews.

Potential FCPA exposure notwithstanding, when assessing risk an organization must look beyond the United States and the FCPA. In the last several years we have seen the emergence of aggressive local anti-corruption legislation and enforcement. Perhaps most representative is the GlaxoSmithKline (GSK) resolution in China. In September 2014, a Chinese subsidiary of GSK was found guilty in Chinese court — after a one-day trial closed to the public — of bribing hospitals and doctors by channelling kickbacks through pharmaceutical associations and travel agencies. Chinese authorities imposed a corporate fine of US$500 million. At the individual level, five Chinese executives of the company were found guilty and received suspended prison sentences.

Companies must protect themselves from corruption risk. Effective compliance programs not only detect and remediate improper conduct, but are also considered by enforcement authorities when negotiating a resolution. In published guidance, the DOJ and SEC advise that the existence and

effectiveness of a corporate compliance program may influence the nature of the resolution, the penalty amount, and the need for a monitor or self-reporting. Furthermore, compliance programs — or lack thereof — have been cited in recent FCPA resolutions. For example, in 2012 the DOJ declined to prosecute Morgan Stanley in large part because of its robust compliance program and internal controls.

In the DOJ press release announcing the guilty plea of the Morgan Stanley's managing director for conspiracy to evade the company's internal controls, the DOJ noted that: Morgan Stanley maintained a system of internal controls meant to ensure accountability for its assets and to prevent employees from offering, promising or paying anything of value to foreign government officials. Morgan Stanley's internal policies, which were updated regularly to reflect regulatory developments and specific risks, prohibited bribery and addressed corruption risks associated with the giving of gifts, business entertainment, travel, lodging, meals, charitable contributions and employment. Morgan Stanley frequently trained its employees on its internal policies, the FCPA and other anti-corruption laws. Between 2002 and 2008, Morgan Stanley trained various groups of Asia-based personnel on anti-corruption policies 54 times. During the same period, Morgan Stanley trained Peterson on the FCPA seven times and reminded him to comply with the FCPA at least 35 times. Morgan Stanley's compliance personnel regularly monitored transactions, randomly audited particular employees, transactions and business units, and tested to identify illicit payments. Moreover, Morgan Stanley conducted extensive due diligence on all new business partners and imposed stringent controls on payments made to business partners.

While the nature and extent of any compliance program must be tailored to specific operational and geographic risk factors, certain steps and components of any effective compliance program are universal. This article provides a step-by-step approach to designing and implementing an anticorruption compliance program.

Step 1: Senior management decides to develop and implement a compliance program

The purpose of a compliance program is tri-fold: to prevent, detect and remediate violations. When successful, compliance programs minimize potential exposure and enforcement scrutiny. To be effective, however, anti-corruption compliance programs must not be ad hoc. For a program to work, it must be purposefully designed and implemented.

Therefore, before going any further, a company must decide to implement a compliance program. As the FCPA guidance emphasizes that a "culture of compliance" starts with "tone at the top," this decision is best made by one or more senior executives with adequate authority. To ensure appropriate oversight, oftentimes a compliance officer is named. Equally important is that a decision to implement a compliance program also requires the assignment of appropriate monetary and personnel resources to the program and a commitment to fully integrate the program throughout the organization.

Step 2: Risk assessment

After a decision to develop compliance program has been made, an organization should conduct a comprehensive baseline risk assessment. The results of the risk assessment will become a road map to developing an effective compliance program. Typically, a risk assessment involves the identification of geographical and operational risk factors. The nature and extent of a risk assessment

will vary considerably based on the size and operations of the organization. Example considerations include:

- *Geographic risk:* Where is the company operating? What is the perceived level of corruption in these countries? Is the company operating in locations where US enforcement authorities are actively working with foreign government authorities to pursue FCPA investigations and prosecutions?
- *Operational risk:* Is the company operating in a sector that has been subject to increased enforcement activity (e.g., energy, logistics, transportation, pharmaceuticals, technology)?
- *Business partners:* To what extent does the company rely on third parties? Do these third parties interact with government officials? Does the company have joint-venture partners? Have there been recent acquisitions? Have the acquired entities been fully integrated? Are there any instances of prior FCPA or other anticorruption non-compliance?

If at all possible, risk assessments should be performed at the direction of legal counsel in order to retain privilege protections. Components of a risk assessment should include some combination of remote questionnaires for low-to-medium risk locations and on-site interviews at higher-risk locations. Once a risk assessment is complete, it is critical that the results are synthesized and analyzed. The methodology and limitations of the assessment should be documented. Likewise, recommendations stemming from the review should be documented and communicated to senior management.

Compliance risk evolves, sometimes quickly. A company must be able to identify new or heighted risk to accommodate an ever-shifting regulatory and enforcement landscape. Separate from the baseline risk assessment discussed above, targeted risk assessments should be a regular — often annual — part of a company's compliance efforts.

Step 3: Design of the compliance program

Once the company has conducted an adequate risk assessment, design of the program can begin. Typically, anti-corruption compliance programs include the following components.

Code of conduct. The code of conduct is the cornerstone of any company's compliance program. The code of conduct should: (1) set forth a strong, clear commitment to lawful and ethical business practice (including an explicit prohibition against corrupt payments); (2) be easily accessible by all employees and agents and available in all languages in which the company does business; and (3) cite to more detailed policies and procedures. Oftentimes, an organization's code of conduct will incorporate quotes or excerpts from senior management regarding a company's commitment to compliance, in an effort to set the "tone at the top."

Anti-corruption policies and procedures. Separate from the code of conduct, internal policies should at a minimum address corruption risks associated with: (1) gifts; (2) travel and lodging; (3) entertainment; (4) meals; (5) charitable and political contributions; and (6) employment.

Policies and procedures also need to account for risks associated with the use of third-party agents by providing for vendor selection and market testing procedures, pre-contracting due diligence, and contractual safeguards, including anti-corruption representations and warranties, and audit rights.

More globally, written components of a compliance program should adopt a clear-line approach. There should be no room to operate in the gray. All bribery, not just bribery of foreign government officials, should be prohibited. Additionally, though the FCPA permits facilitation payments, most local

anti-corruption laws prohibit such payments. A cleaner approach to corporate compliance is to prohibit facilitation payments. Finally, a company's policies and procedures must be regularly reviewed and updated as appropriate.

Training. As a component of any compliance program, regular anti-corruption training addressing specific risk factors should be provided. Training with industry-specific hypotheticals or examples is often effective. Typically, anti-corruption training will be some combination of live, in-person training and Web-based training. Training should be provided for all new hires and at least annually for all employees. Additionally, it may be prudent for a company to provide targeted, supplemental anti-corruption training to employees in high-risk markets or in high-risk business units. Training is an excellent mechanism for two-way communication, where policies are reinforced and employees can raise any areas of concern.

As a complement to annual training, an organization may also wish to consider regular anti-corruption updates. These updates, often sent via email from the compliance or general counsel's office, could summarize a relevant enforcement action or remind employees of the company's compliance program components.

Acknowledgements and certifications. All employees should be required to annually certify their receipt and understanding of anti-corruption training. Additionally, an organization should consider requiring that employees certify their compliance with applicable laws and policies. Such certifications are particularly prudent for those individuals in high-risk or sensitive positions.

Reporting mechanisms. Reporting mechanisms permitting anonymous reporting of incidents of potential misconduct allow for early detection and remediation of potential violations. Reporting potential compliance violations should be mandatory. Additionally, for companies subject to the Sarbanes-Oxley Act of 2002 (SoX), mechanisms allowing for anonymous reporting are required. Examples of mechanisms by which employees can report include: (1) hotline; (2) email or electronic report; (3) communications to the general counsel's or compliance office; (4) communications to direct report or other supervisor. The available reporting mechanisms, including any anonymous reporting mechanisms, should be widely communicated so that all employees know how to report suspected violation.

SoX requires that: Each audit committee shall establish procedures for: (A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters. Sarbanes-Oxley Act of 2002 § 301(4).

Additionally, it is worth noting the tension between strong data privacy jurisdictions — namely, the European Union (EU) — and the SoX reporting requirements. EU data privacy laws often conflict with anonymous hotlines. Examples of hurdles posed by EU data privacy laws include: (1) restrictions against hotlines accepting anonymous tips; (2) restrictions as to the types of violations (subject matter) for which an employee can report anonymously; (3) limits on which employees can use the hotline; (4) preferences regarding whether a hotline be in-house or outsourced; and (5) requirements that a hotline be registered with local data privacy authorities. Because EU data privacy concerns can make implementing a hotline or other anonymous reporting mechanism more complicated, it would be prudent to receive country-specific advice regarding potentially conflicting local laws and regulations should your organization operate in one of these jurisdictions.

Third-parties. It is almost undisputed that third parties present the greatest amount of risk to any compliance program. In fact, it is estimated that more than 90 percent of FCPA enforcement actions involve conduct undertaken by third parties. Accounting for this risk is one of a compliance program's most vital components. One area in which an organization can attempt to mitigate third-party risk, and identify potential red flags, is through pre-contracting anti-corruption due diligence. Examples of red-flags often seen during the course of third-party due diligence include: (1) third party has a history of or reputation for corruption; (2) third party has no expertise for the services it claims to provide; (3) third party requires payment in cash; (4) third party requires that representation be anonymous; (5) third party requests over-invoicing; and (6) third-party operates in a high-risk location or industry.

Joint ventures (JVs), mergers and acquisitions. In the JV and acquisition context, the last thing any organization wants is to learn of is undiscovered FCPA issues. The DOJ has a broad view under which a successor company can be charged with its predecessor's FCPA violations. As it pertains to JVs, an entity that owns a majority interest in a JV is strictly liable for the books and records and internal controls of that JV under the FCPA's accounting provisions. Further, under the FCPA's antibribery provisions, even if an organization is not a majority owner or does not exercise control, it can still be held liable for the conduct if it had knowledge — actual or constructive — of the wrongdoing.

An issuer that owns a minority interest in a joint venture may also be liable under the accounting provisions. However, it may avoid liability by demonstrating that it undertook "good faith efforts" to "use its influence, to the extent reasonable under the issuer's circumstances," to cause the joint venture to implement controls designed to ensure compliance with the accounting provisions. 15 U.S.C. § 78(m)(b)(6).

Because of the significant risk posed by JVs and acquisitions, companies should conduct thorough anti-corruption due diligence on potential acquisition targets and JV partners. Like compliance programs as a whole, due diligence is not one-size-fits-all. The nature and extent of the due diligence necessary depends on specific risks presented and any red flags identified. If reasonably comprehensive due diligence is not possible in advance of a deal, an organization should conduct due diligence immediately following the acquisition or formation of the JV. Post-closing due diligence can look for red flags in invoicing and account payable, reimbursement of travel and entertainment expenses, and analyze key customer relationships. Apart from due diligence, following an acquisition or formation of a JV, the company should ensure that the compliance program is fully integrated. This is often easier said than done but can be accomplished with the right tone at the top, a prompt rollout of policies and procedures, followed up by training.

Integration includes incorporating the "acquired company into all of its internal controls, including its compliance program" and "training new employees, reevaluating third parties under company standards and, where appropriate, conducting audits on new business units." FCPA Guidance at 62.

Step 4: Implementation

Implementation of a compliance program requires effective communication both internally and externally. The program should be implemented globally — as opposed to a phased rollout — with a specific focus on nerve centers and high-risk operations and locations. Oftentimes, a company will have a gold standard compliance program on paper, but fail to communicate its requirements to employees at all levels of the organization. A compliance program is only effective if employees know and understand their obligations, particularly as it applies to an employee's reporting obligations should potential misconduct be discovered. An organization's ability to efficiently detect and appropriately remediate any potential compliance violation is a hallmark of an effective program.

Step 5: Enforcement

Effective compliance programs have teeth. The DOJ and SEC have made clear that “no one should be beyond its reach” — organizations must be willing to remediate and discipline at all levels of the organization. Disciplinary measures should be set forth in applicable policies. When evaluating a company’s response to potential FCPA violations, enforcement authorities will look to the scope of a company’s remediation efforts. A key component of remediation is discipline, including termination, of “bad actors.” No matter how seemingly insignificant, all disciplinary measures should be appropriately documented.

Incentives for compliance should also be considered. The FCPA guidance states that “positive incentives” can “drive compliant behavior.” Examples of incentives could include promotions, and notations in personnel evaluations.

Step 6: Monitoring and evaluation

Compliance programs cannot become stagnant. Continuous, proactive monitoring and evaluation is a hallmark component of any effective compliance program. It is critical that companies be able to adapt to the changing risk landscape. Compliance programs need to be regularly reviewed and assessed, which includes some combination of the following:

- Reviewing policies and procedures with a direct or indirect anticorruption component;
- Reviewing other potentially relevant documents, including incident reports and contracts with high-risk third parties;
- Interviewing individuals in high-risk positions;
- Having relevant individuals certify compliance with anti-corruption policies and procedures;
- Providing supplemental and/or targeted anti-corruption training where appropriate; and
- Providing recommendations of policy or other compliance program enhancement.

Organizations should not wait until an issue arises in one location to react by assessing the effectiveness of its program in other locations. Compliance assessments should have a regular schedule and budget. These assessments should be performed in conjunction with the regular risk assessments discussed above.

Step 7: Responding to potential compliance issues

The DOJ and SEC expect corporate entities to internally respond to and review incidents of reported misconduct. An effective compliance program must have an efficient process to respond to allegations of potential violations. Immediately upon receipt, the allegation should be reviewed and appropriately directed. Complaints should be evaluated for their credibility and seriousness. Credible reports should be further investigated through an internal investigation.

Internal investigations should be directed by legal counsel — either internal or external — so that the investigation can retain privilege protections. Depending on the severity of the reported incident, an investigation may include some combination of:

- *Document review:* A review of potentially applicable policies and procedure and, in more extreme instances, a focused review of relevant employee’s email and other documents provide the investigative team with the necessary information to be able to conduct an

adequate internal investigation. When necessary, a company should also consider whether distribution of a document preservation notice to employees who may have responsive documents would be appropriate.

- *Forensic analysis:* Depending on the nature and scope of the alleged misconduct, it may be appropriate to perform a targeted forensic analysis of the relevant books and records. While forensic analysis is not always required, a forensic analysis may be appropriate where allegations involve falsification or records, circumvention of internal controls, or when a systemic issue is suspected. Whether to use the internal audit function or external auditors to perform this analysis should also be considered.
- *Interviews:* Interviews of employees with potentially relevant information are a key component of an internal investigation and will assist the organization in evaluating the potentially improper conduct.
- *Documentation:* An organization should always document the methodology and findings of an internal investigation. Disciplinary measures and or remedial efforts, if any, should also be documented.

Additionally, reported compliance incidents should be documented, categorized by issue, and regularly synthesized. Much can be gleaned from analyzing trends in reported incidents, including, for example: (1) whether the incident is an outliner or indicative of a systemic issue, (2) whether certain categories of allegations create credibility concerns, and (3) whether controls should be updated to account for frequently-observed issues.

Conclusion

Perhaps no area of international business compliance has received more attention in the last ten years than anti-corruption. Steady and aggressive enforcement of the US FCPA laws continues. It is no longer uncommon to see companies paying in excess of one hundred million dollars in criminal fines and penalties to resolve FCPA or other anticorruption allegations. These enormous monetary resolutions aside, oftentimes the investigative costs a company must incur are higher than the penalties themselves. In addition to being expensive, investigations are lengthy and invasive. Proactively creating and maintaining an anticorruption compliance program may be best defense. However, not all compliance programs are created equally. A one-size-fits-all approach to anti-corruption compliance never works. Companies must create and implement flexible programs that are tailored to the specific needs of the organization and that account for the company's unique risk indicators.

Further Reading

15 U.S.C. §§ 78dd-1 et seq.

15. U.S.C. §78dd-1.

15 U.S.C. § 78m(b)(2)(A); 15 U.S.C. § 78m(b)(2)(B) .

Gibson Dunn & Crutcher 2014 Year-end FCPA Update.

Crim. Div., U.S. DOJ & Enforcement Div., U.S. SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act, 56 (Nov. 14, 2012) (hereinafter "FCPA Guidance") ("In addition to considering

whether a company has self-reported, cooperated, and taken appropriate remedial actions, DOJ and SEC also consider the adequacy.

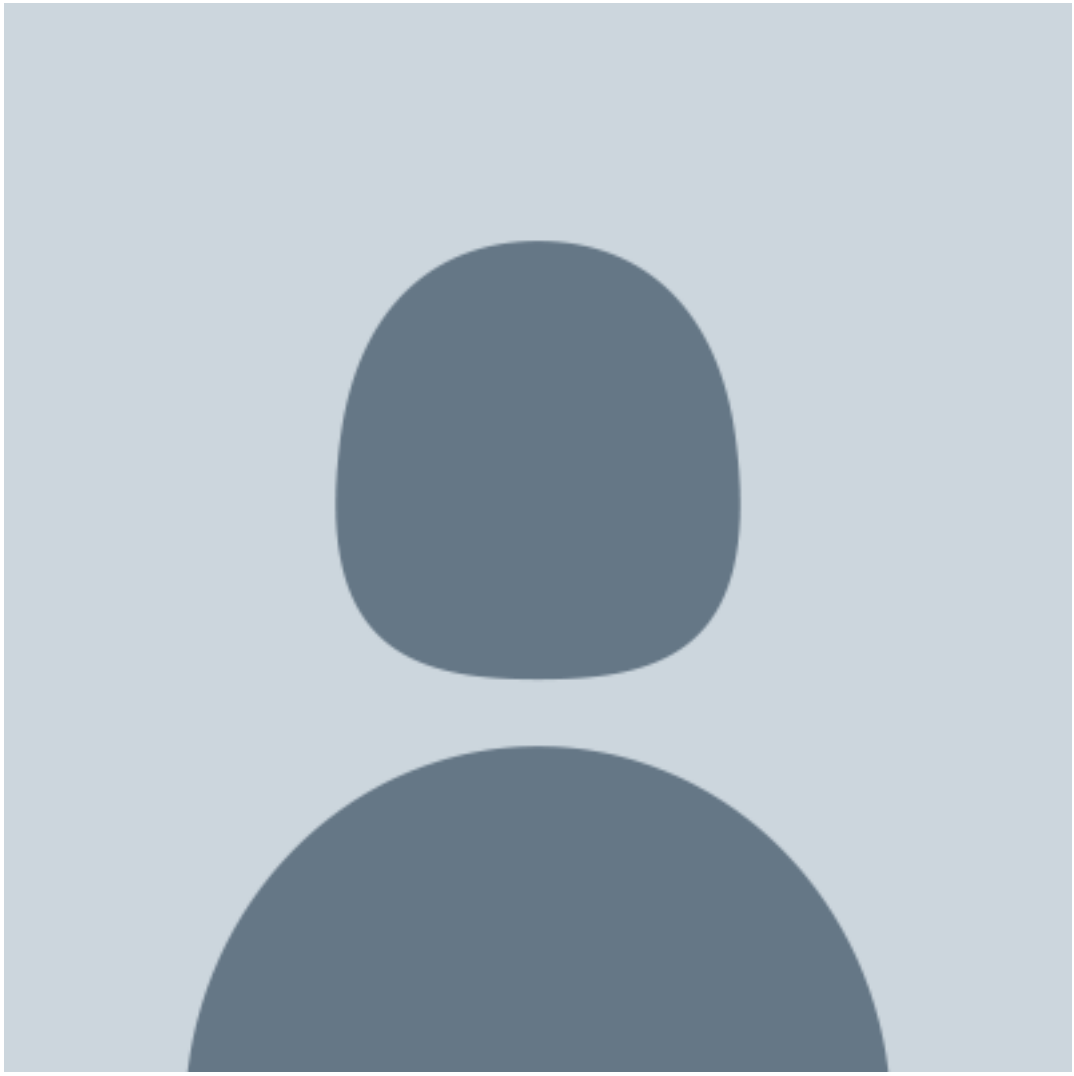
FCPA Guidance at 57.

Opinion Procedure Release No. 08-02 describes that when a Company is unable to conduct through pre-deal due diligence, it can still be rewarded if conducts adequate post-closing due diligence; see also FCPA Guidance at 62.

FCPA Guidance at 59.

FCPA Guidance at 61–62.

Kristen Collier Wright

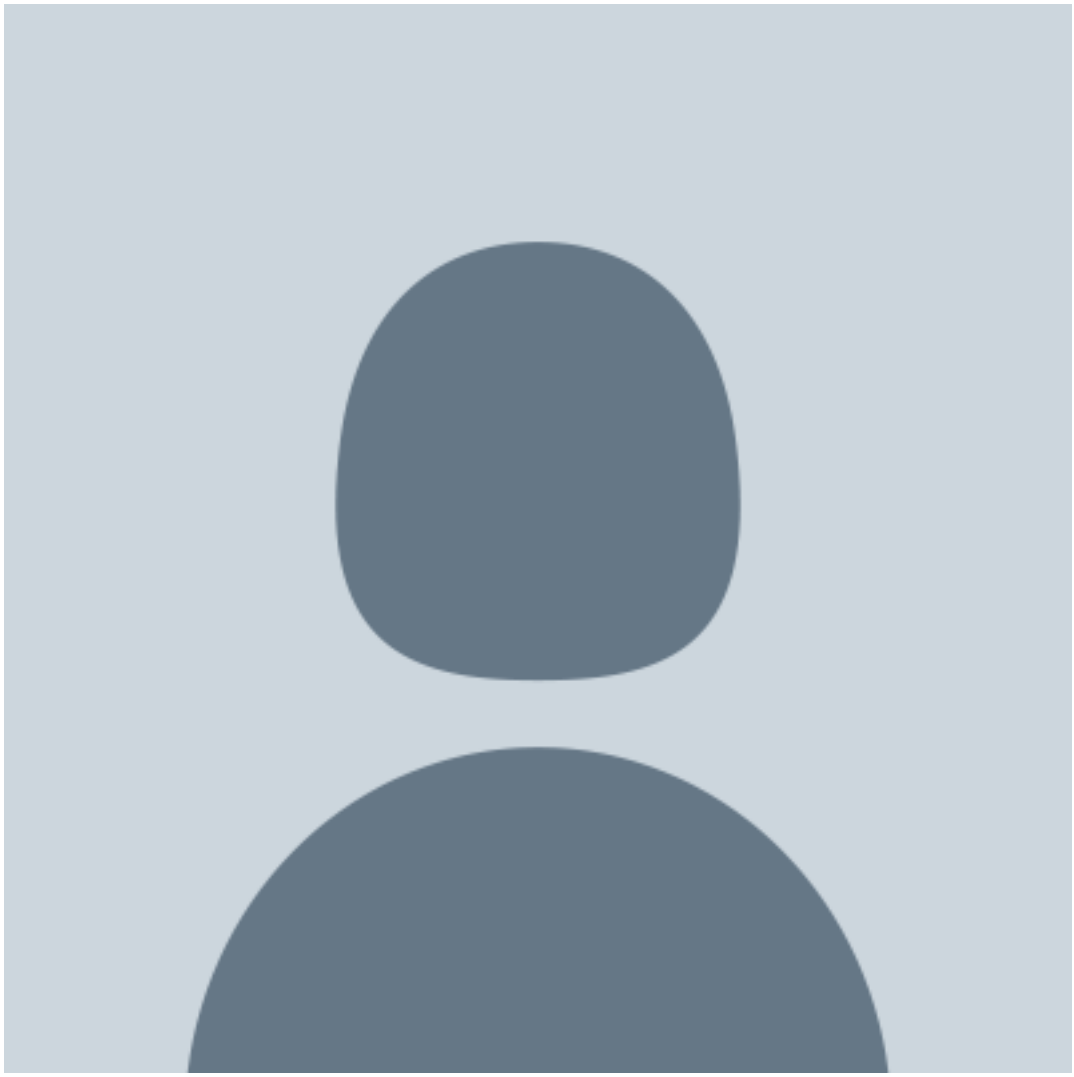


Senior Vice President, General Counsel and Secretary, Customer Satisfaction

AutoZone, Inc.

AutoZone, Inc. is a Fortune 500 company and leading retailer of automotive parts and products. AutoZone has more than 75,000 employees and operates in 49 states, Puerto Rico, Mexico and Brazil. Wright serves on AutoZone’s executive committee and oversees the legal department, government affairs, corporate communications and community relations.

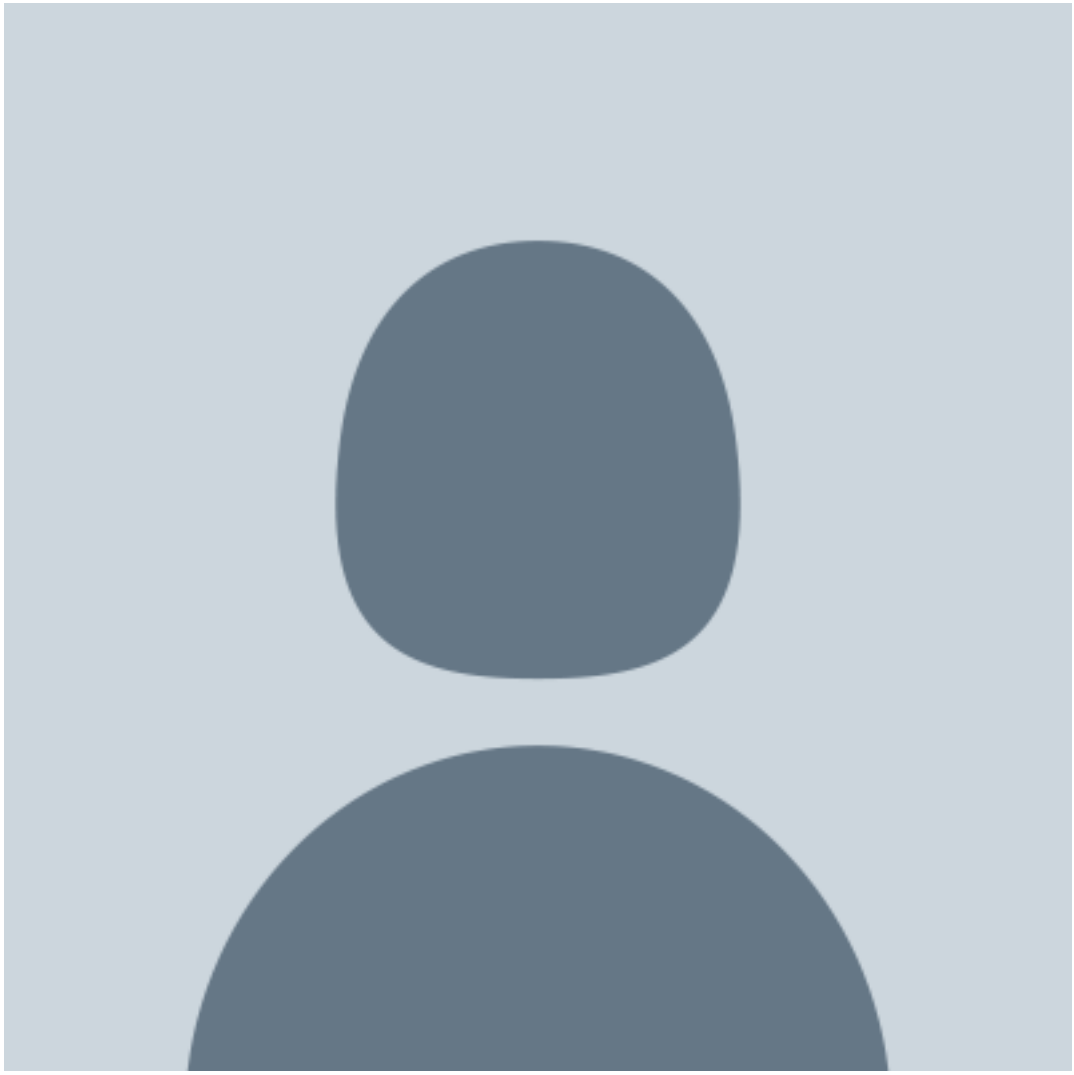
Wallace W. Dietz



Chair of the Compliance and Government Investigations (CGI) Practice Group

Wallace W. Dietz works in the firm’s Nashville and Washington, DC offices. He has more than 30 years of experience guiding his clients through complex litigation and investigations and has conducted anti-corruption investigations on four continents.

Lindsey Brown Fetzer



Associate

the Washington, DC office of Bass, Berry & Sims PLC

Lindsey Brown Fetzer focuses her practice on white collar and corporate compliance matters. She has experience in matters involving the FCPA and has conducted internal investigations and risk-based anti-corruption compliance reviews throughout Asia, Europe and South America.