

The Five Essential Elements of a Corporate Compliance Program - Part II

Tuesday morning, at the University Club of Chicago, Stephen Martin and I will co-present at a Foreign Corrupt Practices Act (FCPA) event hosted by Kreller. If you are in or near Chicago, I hope that you can join us for this presentation. The title of our presentation is “Anti-Corruption/FCPA Developments & Best Practices” and we will focus on a concept that Stephen and his partners at the law firm of Baker & McKenzie have developed which are five essential elements of a corporate compliance program. In Part I, I discussed the background to the development of the five essential elements. In today’s installment, Part II, I will detail the remaining elements in the five elements of an essential compliance program.

III. Standards and Controls

Generally, every company has three levels of standards and controls. (1) Code of Conduct. Every company should have a Code of Conduct which should express its ethical principles. However, a Code of Conduct is not enough. (2) Standards and Policies. Every company should have standards and policies in place that build upon the foundation of the Code of Conduct and articulate Code-based policies, which should cover such issues as bribery, corruption and accounting practices. (3) Procedures. Every Company should then ensure that enabling procedures are implemented to confirm those policies are implemented, followed and enforced. FCPA compliance *best practices* now require companies to have additional standards and controls, including, for example, detailed due diligence protocols for screening third-party business partners for criminal backgrounds, financial stability and improper associations with government agencies. Ultimately, the purpose of establishing effective standards and controls is to demonstrate that your compliance program is more than just words on a piece of paper.

IV. Training

Another pillar of a strong compliance program is properly training 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. The Department of Justice’s (DOJ) expectations of effectiveness are measured by who a company trains, how the training is conducted and how often training occurs.

There are several key elements to training. First is that you need to train the right people. You must prioritize which audience to educate by starting your training program in higher risk markets and focus on directors, officers and sales employees who may have direct contact with government officials or deal with state-owned entities. Again, focus initially on training country managers in your company’s high-risk markets, then expand geographically and through the ranks of employees.

Second, in high risk markets and for high risk employees or third parties you should conduct live, annual training. Enforcement officials have made it clear that live, in-person training is the

preferred method in high-risk markets and also that it should be regular and frequent. Another benefit of live training is the immediate feedback from employees that would be much less likely to occur during a webinar or other remote training. Lastly, during live training, employees are more likely to make casual mention of a potentially risky practice, giving you the opportunity to address it before it becomes a larger problem.

It is important that you pay attention to what employees say during training. This is 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 red flags and uncover issues that should be reviewed and addressed quickly.

Thirdly, you should tailor your training to each country. This means that employing a generic script for compliance training is a mistake. To be effective, training programs should be customized by region, country, industry, areas of compliance and types of employee. In addition to Foreign Corrupt Practices Act (FCPA), UK Bribery Act, and OECD guidelines, focus on compliance risks in the country where the employees being trained are working. For example: In China, address the many corruption risks involved in dealing with state-owned entities.

V. Oversight - including monitoring, auditing and responses

The issue your company should focus on here is whether employees are staying with the compliance program. Even after all the important ethical messages from management have been communicated to the appropriate audiences and key standards and controls are in place, there should still be a question of whether the company's employees are adhering to the compliance program. Two of the seven compliance elements in the US Sentencing Guidelines call for companies to monitor, audit and respond quickly to allegations of misconduct. These three highlighted activities are key components enforcement officials look for when determining whether companies maintain adequate oversight of their compliance programs.

Many companies fall short on effective monitoring. This can sometimes be attributed to confusion about the differences between monitoring and auditing. **Monitoring** is a commitment to reviewing and detecting compliance programs 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. **Auditing** is a more limited review that targets a specific business component, region or market sector during a particular timeframe in order to uncover and/or evaluate certain risks, particularly as seen in financial records. However, you should not assume that because your company conducts audits that it's effectively monitoring. A robust program should include separate functions for auditing and monitoring. While unique in protocol, however, the two functions are related and can operate in tandem. Monitoring activities can sometimes lead to audits. For instance if you notice a trend of suspicious payments in recent

monitoring reports from Indonesia, it may be time to conduct an audit of those operations to further investigate the issue.

Your company should establish a regular monitoring system to spot issues and address them. Effective monitoring means applying a consistent set of protocols, checks and controls tailored to your company's risks to detect and remediate compliance problems on an ongoing basis. To address this, your compliance team should be checking in routinely with local finance departments in your foreign offices to ask if they've noticed recent accounting irregularities. Regional directors should be required to keep tabs on potential improper activity in the countries they manage. Additionally the global compliance committee should meet or communicate as often as every month to discuss issues as they arise. These ongoing efforts demonstrate your company is serious about compliance.

Finally, as was emphasized again with the recent Pfizer Deferred Prosecution Agreement (DPA), your company should establish protocols for internal investigations and disciplinary action. The Pfizer "Enhanced Compliance Obligations" included the following on investigative protocols: (a) On-site visits by an FCPA review team comprised of qualified personnel from the Compliance, Audit and Legal functions who have received FCPA and anti-corruption training; (b) Review of a representative sample, appropriately adjusted for the risks of the market, of contracts with, and payments to, individual foreign government officials or health care providers, as well as other high-risk transactions in the market; (c) Creation of action plans resulting from issues identified during the proactive reviews; these action plans will be shared with appropriate senior management and should contain mandatory remedial steps designed to enhance anti-corruption compliance, repair process weaknesses, and deter violations; and (d) a review of the books and records of a sample of distributors which, in the view of the FCPA proactive review team, may present corruption risk. Prior to such an investigation, however, the company should have procedures - including document preservation protocols, data privacy policies, and communication systems designed to manage and deliver information efficiently - in place to make sure every investigation is thorough and authentic.

Finally, and consistent with Stephen Martin's Baker & McKenzie partner Paul McNulty's Maxim Three (What did you do about it?), is your remediation efforts. Your company should remediate problems quickly. A key concept behind the oversight element of compliance is that if companies are policing themselves on compliance-related issues, the government won't have to do it for them. Remediation, then, is an important component of oversight. If your company's sales force in Thailand is engaged in potentially improper activity due to a lack of adequate training, remediate the deficiency and schedule that training now. In the end, it's 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.

Stephen Martin and the Baker & McKenzie team have put together an excellent resource for the compliance practitioner in their five essential elements of a corporate compliance program. I

hope that you can attend our FCPA event this week. For those of you who cannot attend in person, you can email me for the slide deck and other materials after the event.

This publication contains general information only and is based on the experiences and research of the author. The author is not, by means of this publication, rendering business, legal advice, or other professional advice or services. This publication is not a substitute for such legal advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified legal advisor. The author, his affiliates, and related entities shall not be responsible for any loss sustained by any person or entity that relies on this publication. The Author gives his permission to link, post, distribute, or reference this article for any lawful purpose, provided attribution is made to the author. The author can be reached at tfox@tfoxlaw.com.

© Thomas R. Fox, 2012