Doing Compliance: Design, Create, and Implement an Effective Anti-Corruption Compliance Program

THOMAS FOX

COMPLIANCE WEEK PUBLISHED BY ark GROUP

Doing Compliance: Design, Create, and Implement an Effective Anti-Corruption Compliance Program

COMPLIANCE WEEK ark GROUP

COMPLIANCE WEEK
77 N. Washington Street, 4th Floor
Boston
MA 02114
Tel +1 888 519 9200
Fax +44 (0)20 7324 2373
info@complianceweek.com

ARK CONFERENCES LTD
6-14 Underwood Street
London N1 7JQ
United Kingdom
Tel +44 (0)20 7566 5792
Fax +44 (0)20 7324 2373
publishing@ark-group.com

COMPLIANCE WEEK
Editor and Publisher
Matt Kelly
mkelly@complianceweek.com

Head of Sales and Marketing
Donna Rice
drice@complianceweek.com

ARK GROUP
Head of Content Strategy
Fiona Tucker
fiona.tucker@wilmington.co.uk

Reports Content Manager
Helen Roche
helen.roche@wilmington.co.uk

Assistant Editor
Laura Slater
laura.slater@ark-group.com

ISBN:
978-1-78358-159-7 (hard copy)
978-1-78358-160-3 (PDF)

Copyright
The copyright of all material appearing within this publication is reserved by the authors and Ark Conferences 2014. It may not be reproduced, duplicated or copied by any means without the prior written consent of the publisher.

Online bookshop
www.ark-group.com/bookshop

Contents

Executive summary VII

About the author XIII

Acknowledgements XV

Chapter 1: Where it all begins – Commitment from senior management and a clearly articulated policy against corruption 1
At the top 3
In the middle 5
Tone at the bottom 7

Chapter 2: Some written controls 11
Standards of conduct, policies, and procedures (a code of conduct) 11
Code of conduct 13
Policies, procedures, and controls 17
Revising your code of conduct, policies, and procedures 19

Chapter 3: For the CCO – Oversight, autonomy, and resources 23
Autonomy 23
The board 25
20 questions directors should ask about compliance committees 29
Resources 31

Chapter 4: The cornerstone of your compliance program – Risk assessments 37
What should you assess? 38
How should you assess your risks? 41
The desktop risk assessment 42
Engage and educate: A different model for a risk assessment 45
How do you evaluate a risk assessment? 47

Chapter 5: Getting out on the road – Training and continuous advice 51
Training 51
Evaluation of FCPA compliance training 54
End of training "flea dip" 55
Training to resist a bribe 56
Communication 58

Chapter 6: Do as I do and as I say – Hiring, incentive, and disciplinary measures 63
Compliance due diligence checks: The reference interview 65
Using HR to change your company's compliance DNA 66
Succession planning from the compliance perspective 69
The fair process doctrine as a key component of a compliance program 71
Implementing compliance incentives 73

Chapter 7: Your greatest source of FCPA risk 77
Step 1: Business justification 78
Step 2: Questionnaire 80
Step 3: Due diligence 83
Step 4: The contract 93
Step 5: Management of the relationship 98
Some final thoughts 103

Chapter 8: How do I love thee – Confidential reporting and internal investigations 107
How does your organization treat whistleblowers? 109
What is your FCPA investigation protocol? 112
Use of specialized counsel in a FCPA investigation 113

Chapter 9: How to get better 117
Six steps to implementing continuous monitoring in your compliance program 119
You have a strategic plan; now what do you do? 121
The regulator's perspective 122

Chapter 10: Should I or shouldn't I? Mergers and acquisitions 125
Pre-acquisition risk assessment 126
A five-step process for pre-acquisition due diligence 127
What should you do with the information that you uncover in your pre-acquisition due diligence? 130

Chapter 11: A few words about facilitation payments 137
The statute 138
Enforcement actions and a declination 139
Some guidance 140

Chapter 12: Conclusion 143

Index 145

Executive summary

THE US Foreign Corrupt Practices Act (FCPA) has been around since 1977. However, the last ten years has seen an explosion of growth in FCPA enforcement with both the number of enforcement actions far exceeding what occurred in the first 25 years of the FCPA and fines and penalties headed into near stratospheric levels. In 2011, the UK enacted into law the UK Bribery Act, which incorporates some of the concepts present in the FCPA along with some components not included in the FCPA, such as making "private-to-private" bribery illegal. While there have not been any significant prosecutions under the UK Bribery Act to-date, the UK Serious Fraud Office (SFO) has announced that several companies and individuals are under investigation. In 2013, the Chinese government announced a massive investigation into the UK Company GlaxoSmithKline PLC (GSK) for bribery and corruption under Chinese domestic law, marking the first time Chinese authorities have investigated a western company under Chinese domestic law.

It is clear that enforcement actions against bribery and corruption are not going to go away – or even lessen – in the future. Just as the world is becoming increasingly 'flat' for business and commercial operations, the same is true for anti-corruption and anti-bribery enforcement. Any company that does business internationally must be ready to deal with a business environment which has these new realities. While there are several excellent books about the FCPA and anti-corruption enforcement, very few deal with the "how" of doing business in this new enforcement milieu.

This book is designed to be a one-volume work, which will provide you with the basics of how to create and maintain an anti-corruption and anti-bribery compliance program to suit any business climate across the globe. I have based my discussion of a best practices compliance program on what

the Criminal Division of the US Department of Justice (DOJ) and Enforcement Division of the Securities and Exchange Commission (SEC) set out in their jointly produced "FCPA – A Resource Guide to the US Foreign Corrupt Practices Act", which includes FCPA Guidance on the ten "hallmarks" of an effective compliance program.

The FCPA Guidance wisely makes it clear that it is impossible to take a blanket approach to compliance: "Individual companies may have different compliance needs depending on their size and the particular risks associated with their businesses, among other factors. When it comes to compliance, there is no one-size-fits-all program. Thus, the discussion below is meant to provide insight into the aspects of compliance programs that DOJ and SEC assess, recognizing that companies may consider a variety of factors when making their own determination of what is appropriate for their specific business needs. Indeed, small- and medium-size enterprises likely will have different compliance programs from large multi-national corporations, a fact DOJ and SEC take into account when evaluating companies' compliance programs."

This book does not discuss the underlying basis of the FCPA or any other anti-corruption or anti-bribery legislation. I have assumed the reader will have a modicum of knowledge of these laws. If not, several excellent works can provide that framework. This book is about how to do business in compliance with these laws. Like all Americans, I appreciate any list that is deca-based, so the format of 10 hallmarks resonates with me. Accordingly, I have kept this basic organization in laying out what I think you should consider in your anti-corruption and anti-bribery compliance program. In addition to presenting my own views on these areas, I also set out the views of both FCPA practitioners and commentators from other areas of business study and review.

Compliance begins at the top, what should management say and do? "Tone at the top" is a great buzz phrase, but how does a company truly get the message of compliance down through the ranks? The first chapter of this report will discuss the techniques management can use to move the message of compliance down through middle management and into the lower ranks of the company.

The backbone of your anti-bribery compliance program is set out in your written standards and controls, which consist of a code of conduct, compliance policy, and implementing procedures. Chapter 2 will discuss what should be in the written basics of your compliance program and how best to implement these controls.

Chapter 3 focuses on the chief compliance officer (CCO), whose role and function in any compliant organization cannot be overstated. Simply naming a CCO is no longer enough to meet even the minimum requirements of best practices. This chapter will review the compliance function, oversight, autonomy, and resources. One of the key areas that the DOJ will review is how a CCO is allowed to fulfill this role. Does the position have adequate resources? Does it have autonomy and support in the corporate environment? Does the board of directors exercise appropriate oversight? This section will set out how to structure your best practices for the compliance function in an organization.

Chapter 4 covers the cornerstone of your compliance program: your risk assessment. It all begins here. A risk assessment is the road map to managing your risk. The implementation of an effective compliance program is more than simply following a set of accounting rules or providing effective training. Compliance issues can touch many areas of your business, and you need to know not only what your highest risks are, but also where to marshal your efforts in moving forward. A risk assessment is designed to provide a big picture of your overall compliance obligations and then to identify areas of high risk so that you can prioritize your resources to tackle these high-risk areas first.

Once you have designed and implemented your compliance program, the real work begins. Chapter 5 discusses the training you must provide on the compliance program and the continuing advice that must be given to your company thereafter. This means that 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. However, merely conducting training usually is not enough. Enforcement officials want to be certain the messages in the training actually get through to employees. The DOJ's expectations for effectiveness are measured by who a company trains, how the training is conducted, and how often training occurs. In this chapter, you will learn how to get your message of compliance out to your employees.

Any effective compliance program will use a variety of tools to help ensure that it is followed. This means that you must employ both the carrot of incentives and the stick of disciplinary measures to further compliance, as discussed in Chapter 6 of this report. How can you burn compliance into the DNA of your company? Discipline has long been recognized as an important aspect of a compliance regime, but more is now required. In this chapter you will learn

how to structure compliance into the fabric of your company through hiring and promotion of personnel committed to compliance, and how to reward them for doing business ethically and in compliance with the FCPA.

Chapter 7 covers third parties – universally recognized as the highest risk in any compliance program. Indeed, it is estimated that well over 90 per cent of all FCPA enforcement actions involve third parties. Therefore, it is important for an anti-corruption program to manage this highest risk. In this chapter, I will detail a five-step process for the investigation and management of any third party relationship, from agents in the sales chain to vendors in the supply chain.

In any company, your best source of information about not only the effectiveness of your compliance program, but also concerning any violations, is your own employees. This means that you must design and implement a system of confidential reporting to get your employees to identify issues, and then have an effective internal investigation of any issues brought to your attention. Your own employees can be your best defense to prevent a compliance issue from becoming a FCPA violation. In Chapter 8, you will learn about the best practices for setting up internal reporting and investigating claims of compliance violations.

Once you have everything up and running, you still need to oil and update the machine of compliance. Chapter 9 explains how you can do this through the step of continuous improvement, which is the use of monitoring and auditing to review and enhance your compliance regime going forward. A company should focus on 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.

The last thing you want to bring in through an acquisition is another company's FCPA violation for which your company must pay. In Chapter 10, you will learn how to use the mergers & acquisition (M&A) function to proactively manage compliance. Companies do not want to "buy a FCPA violation". Effectively managing your M&A process can help you to identify risk areas in a potential acquisition and then remediate any issues in the post-acquisition integration phase. This section will provide the DOJ's most recent pronouncements on how to avoid FCPA exposure in this key area of corporate growth.

One of the key differences between the US FCPA and UK Bribery Act is that the US law allows facilitation payments. However, in today's interconnected world, to allow one part of your company to make facilitation payments while UK subsidiaries or others covered by the UK Bribery Act are exempt from your standard on facilitation payments can become an administrative nightmare. The concluding chapter of this report will explore what facilitation payments actually are, and in what ways the policing of your internal policy has become more difficult. The chapter will also look at some companies which have been investigated regarding their facilitation payments, and will provide guidelines for you to follow should your company decide to allow these going forward.

About the author

THOMAS FOX has practiced law for over 30 years. He has been a trial lawyer in private practice, a general counsel in the corporate world, and is now recognized as one the leading experts on the Foreign Corrupt Practices Act (FCPA) and compliance programs relating to both the FCPA and other anti-corruption laws. He is the author of two prior award-winning books on the FCPA: *Lessons Learning on Compliance and Ethics* and *Best Practices Under the FCPA and UK Bribery Act*. He blogs daily on all things FCPA on his award winning blogsite, *The FCPA Compliance and Ethics Blog*, and podcasts on all things anti-corruption on *The FCPA Compliance and Ethics Report*. Fox writes for a variety of anti-corruption compliance magazines and publications, and is a featured columnist for *Compliance Week*. He can be reached at tfox@tfoxlaw.com.

Acknowledgements

THIS BOOK could not have come to fruition without the work of several very dedicated professionals who were instrumental in getting it to press, including Matt Kelly, publisher of *Compliance Week*, and Helen Roche from the Ark Group. The group of compliance professionals I look to for guidance in understanding the nuts and bolts of compliance is long and includes such compliance luminaries as Howard Sklar, Henry Mixon, Mike Volkov, Matt Ellis, Stephen Martin, the FCPA Professor (aka Mike Koehler), Paul McNutly, Joe Oringel, Jay Martin, Dan Chapman, Jonathan Marks, Scott Moritz, Diana Lutz, Bill Athanas, David Simon, Aaron Murphy, Jim McGrath, and Jay Rosen. These and many others have been very generous with their time in sharing with the greater compliance community. Their writing and speaking on topics related to compliance have helped to inform me on what constitutes an effective compliance program. Finally, and certainly for me most importantly, my editor and wife, Michele Rudland, for not only doing the slog work of editing but for putting up with me throughout this process.

Chapter 1: Where it all begins – Commitment from senior management and a clearly articulated policy against corruption

"TONE AT the top" has become a phrase inculcated in the compliance world. The reason it is so important to any compliance program is because it *does actually matter*. Any compliance program starts at the top and flows down throughout the company. The concept of appropriate tone at the top is in the US Sentencing Guidelines for organizations accused of violating the FCPA; the FCPA Guidance; the UK Bribery Act's Six Principles of Adequate Procedures; and the OECD Good Practice Guidance on Internal Controls, Ethics and Compliance (OECD Good Practices). The reason all of these guidelines incorporate it into their respective practices is that all employees look to the top of the company to see what is important. Or, to follow my colleague Mike Volkov in quoting Bob Dylan, "You don't need to be a weatherman to know which way the wind blows."

The US Sentencing Guidelines reads: "High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program… and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law."

The OECD Good Practices recommends: "…strong, explicit and visible support and commitment from senior management to the company's internal controls, ethics and compliance programs or measures for preventing and detecting foreign bribery…"

> Principle 2 of the Guidance to the UK Bribery Act reads: "The top-level management of a commercial organisation (be it a board of directors, the owners or any other equivalent body or person) are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable."

The FCPA Guidance, under the section entitled "Commitment from Senior Management and a Clearly Articulated Policy Against Corruption", states, "Within a business organization, compliance begins with the board of directors and senior executives setting the proper tone for the rest of the company. Managers and employees take their cues from these corporate leaders. Thus, DOJ and SEC consider the commitment of corporate leaders to a 'culture of compliance' and look to see if this high-level commitment is also reinforced and implemented by middle managers and employees at all levels of a business."

However, the DOJ and SEC expect senior management to do more than say the right things. They both expect that such a message will be pushed down the ranks of an enterprise so that "A strong ethical culture directly supports a strong compliance program. By adhering to ethical standards, senior managers will inspire middle managers to reinforce those standards. Compliant middle managers, in turn, will encourage employees to strive to attain those standards throughout the organizational structure. In short, compliance with the FCPA and ethical rules must start at the top. DOJ and SEC thus evaluate whether senior management has clearly articulated company standards, communicated them in unambiguous terms, adhered to them scrupulously, and disseminated them throughout the organization."

The FCPA world is riddled with cases where the abject failure of any ethical "tone at the top" led to enforcement actions and large monetary settlements. In the two largest monetary settlements of enforcement actions to date, concerning Siemens and Halliburton (for the actions of its former subsidiary KBR) respectively, the government specifically noted the companies' pervasive tolerance for bribery. In the Siemens case, for example, the SEC noted that the company's culture "had long been at odds with the FCPA" and was one in which bribery "was tolerated and even rewarded at the highest levels". Likewise, in the Halliburton matter, the government noted that "tolerance of the offense by substantial authority personnel was pervasive" throughout the organization.

At the top

So how can a company overcome these employee attitudes and set, or re-set, its "tone at the top"? In a 2008 speech to the State Bar of Texas Annual Meeting, reprinted in *Ethisphere*, Larry Thompson, PepsiCo executive vice president (EVP) of governmental affairs, general counsel (GC), and secretary, discussed the work of Professor Lynn Sharp at Harvard. From Professor Sharp's writings, Mr Thompson cited five factors which are critical in establishing an effective integrity program and setting the right "tone at the top":

1. The guiding values of a company must make sense and be clearly communicated;
2. The company's leader must be personally committed and willing to take action on the values;
3. A company's systems and structures must support its guiding principles;
4. A company's values must be integrated into normal channels of management decision-making and reflected in the company's critical decisions; and
5. Managers must be empowered to make ethically sound decisions on a day-to-day basis.

David Lawler, writing in his book, *Frequently Asked Questions in Anti-Bribery and Corruption*, boiled it down as follows: "Whatever the size, structure or market of a commercial organization, top-level management's commitment to bribery prevention is likely to include communication of the organization's anti-bribery stance and appropriate degree of involvement in developing bribery prevention procedures." Lawler went on to provide a short list of points that he suggests senior management follow in order to communicate the tone of the company and its attitude toward anti-corruption, as follows:

- Reject a "do as I say, not as I do" mentality;
- Don't just "talk-the-talk" but "walk-the-walk" of compliance;
- Oversee creation of a written statement of a zero tolerance towards bribery and corruption;
- Appoint and fully resource, with money and headcount, a chief compliance officer (CCO);
- Oversee the development of a code of conduct and a written compliance program implementing it;

- Ensure there are compliance metrics on all key business reports;
- Provide leadership to middle managers to facilitate filtering of the zero tolerance message down throughout the organization;
- Don't just have a whistleblowing, reporting, or speak up channel, but celebrate it;
- Keep talking about doing the right thing; and
- Make sure that you are seen providing your CCO with access to you and to the board of directors.

Coming at it from a different perspective, author Martin Biegelman provides some concrete examples in his book, entitled *Building a World Class Compliance Program – Best Practices and Strategies for Success*. He begins the chapter discussed here with the statement "The road to compliance starts at the top." There is probably no dispute that a company takes on the tone of its top management. Biegelman cites a list used by Joe Murphy regarding actions a CEO can take to demonstrate the requisite tone from the "captain's chair" of any business. The list is as follows:

1. Keep a copy of the constitution on your desk: Have a dog-eared copy of your company's code of conduct on your desktop and be seen using it.
2. Clout: Make sure your compliance department has authority, influence, and budget within the company. Have your chief compliance officer report directly to the board of directors.
3. Make them accountable: At senior executive meetings, have each participant report on what they have done to further the compliance function in their business unit.
4. Sticks and carrots: Have both sanctions for violation of company compliance and ethics policies and incentives for doing business in a compliant manner.
5. Don't do as I say, do as I do: Turn down an expensive dinner or trip offered by a vendor. Pass on a gift that you may have received. Turn down a transaction based upon ethical considerations.
6. Be a student: Be seen at intra-company compliance training. Take a one- or two-day course or attend a compliance conference outside your organization.
7. Award compliance: You should recognize outstanding compliance efforts with companywide announcements and awards.

8. The board: Recruit a nationally known compliance expert to sit on your company's board and chair the audit or compliance committee.
9. Independent review: Obtain an independent, outside review of your company's compliance program and report the results to the board's audit committee.
10. Vendors: Mandate that all vendors in your supply chain embrace compliance and ethics as a business model. If not, pass on doing business with them.
11. Network: Talk to others in your industry and your peers about how to improve your company's compliance efforts.

Many companies struggle to come up with some type of metric which can be used by upper management regarding compliance and communication of a company's compliance values. One technique might be to require the CEO to post company-wide emails or other communications once a quarter on some compliance-related topic. The CEO would also be required to email their senior management a minimum of once per quarter on a compliance-related topic. One can cascade this down through the company as far as is practicable. Reminders can be set for each communication so that all personnel know when it is time to send out the message. If these communications are made in a timely manner, this metric has been met.

In the middle

However, a company must have more than simply a good "tone at the top"; it must move the message down through the organization, from senior management to middle management, and into its lower ranks. This means that one of the tasks of any company, including its compliance organization, is to get middle management to respect the stated ethics and values of a company, because if they do so, this will be communicated down through the organization.

Adam Bryant explored this in a *New York Times* interview with Victoria Ransom, the CEO of Wildfire, a company which provides social media marketing software.[1] Ransom spoke about the role of senior management in communicating ethical values, saying, "Another lesson I've learned as the company grows is that you're only as good as the leaders you have underneath you. And that was sometimes a painful lesson. You might think that because you're projecting our values, then the rest of the company is experiencing the values." These senior managers communicate what the

company's ethics and values are to middle management. So while tone at the top is certainly important in setting a standard, Ransom came to appreciate that it must move downward through the entire organization. Bryant wrote that Ransom came to realize "that the direct supervisors become the most important influence on people in the company. Therefore, a big part of leading becomes your ability to pick and guide the right people."

Ransom said that, when the company was young and small, they tried to codify their company values, but they did not get far in the process "because it felt forced". As the company grew, she realized that their values needed to be formalized and stated for a couple of reasons. The first was because they wanted to make it clear what was expected of everyone and "particularly because you want the new people who are also hiring to really know the values". Another important reason was that they had to terminate "a few people because they didn't live up to the values. If we're going to be doing that, it's really important to be clear about what the values are. I think that some of the biggest ways we showed that we lived up to our values were when we made tough decisions about people, especially when it was a high performer who somehow really violated our values, and we took action." These actions to terminate had a very profound effect on the workforce. Ransom said that "it made employees feel like, 'Yeah, this company actually puts its money where its mouth is.'"

Ransom sought to ensure that everyone knew what senior management considered when determining whether employees were "living up to the company culture". The process started when she and her co-founder spent a weekend writing down what they believed the company's values were. Then they sat down with the employees in small groups to elicit feedback. Her approach was to look for what they wanted in their employees. They came up with six qualities:

- Passion: Do you really have a thirst and appetite for your work?
- Humility and integrity: Treat your co-workers with respect and dignity.
- Courage: If you have a great idea, tell us, and if you disagree with people in the room, speak up.
- Curiosity: Constantly question and learn, not only about the company, but about the industry.
- Impact: Are you having an impact at the company?
- Be outward-looking: Do good and do right by each other.

Ransom had an equally valuable insight when she talked about senior management and ethical values. She believes that "the best way to undermine a company's values is to put people in leadership positions who are not adhering to the values. Then it completely starts to fall flat until you take action and move those people out, and then everyone gets faith in the values again. It can be restored so quickly. You just see that people are happier."

What should the tone in the middle be? Put another way, what should middle management's role be in the company's compliance program? This role is critical because the majority of company employees work most directly with middle, rather than top, management; consequently, they will take their cues from how middle management respond to a situation. Moreover, middle management must listen to the concerns of employees. Even if middle management cannot effect a direct change, it is important that employees have an outlet to express their concerns. Therefore your organization should train middle managers to enhance listening skills in the overall context of providing training for what Ransom termed their "manager's toolkit". This is particularly true if there is a compliance violation or other incident which requires some form of employee discipline. Ransom believes that most employees think it important that there be "organizational justice" so that people believe they will be treated fairly. Ransom further explained that without organizational justice, employees typically do not understand or accept outcomes, but if there is perceived procedural fairness then an employee is more likely accept a decision that they may not like.

Tone at the bottom

Even with a great tone at the top and in the middle, you cannot stop there. One of the greatest challenges for a compliance practitioner is how to affect the 'tone at the bottom'. In an article in the *MIT Sloan Management Review*, authors Jules Goddard, Julian Birkinshaw and Tony Eccles looked at this issue when they explored the idea that the "often overlooked, critical source of differentiation is [a] company's beliefs".[2]

One of the questions that the authors answer is: how do we tap into this belief system? They recommend a structured manner of obtaining this information. By using these techniques, they believe that companies can rethink their "basic assumption and beliefs" and identify new directions for their organization. The authors listed seven approaches that they have used, and which I believe that the compliance practitioner can usefully employ to not only determine "tone at the

bottom", but also to make an impact on that tone. They are as follows:

1. Assemble a group: You need to assemble a group of employees who are familiar with the challenges of doing business in a compliant manner in certain geographic regions. Include both long-time employees and those who are relatively new to the organization. The authors also suggest that if you have any employees who have worked for competitors or for other organizations in your industry you include them as well.
2. Ask questions: You should ask the members of this group to articulate their basic assumptions about your compliance model, the management model, your company's business model, and about the future of the industry in general. Ask them to do this individually and not as a group.
3. Categorize the responses: Now comes the work by the compliance practitioner or compliance team, as the authors believe that these assumptions will usually fall into two groups. The first is assumptions that everyone agrees upon the common beliefs. The second is those assumptions that only a few of the participants will identify – this is what the authors call the "uncommon beliefs".
4. Develop tests for common beliefs: For those beliefs that are labeled "common" – you should consider how you know these to be true. The authors caution that simply because the group may believe that the company operates in a common industry or that we "do it because it has always been done this way" that does not necessarily make it a "hard fact". Consider what checks you could perform to verify a common belief. The authors note that the purpose here is to "identify the 'common nonsense' beliefs that everyone holds that are not actually hard laws of nature".
5. Develop tests for uncommon beliefs: Here the authors suggest that you need to consider why some people think that these beliefs are true. What is the information or experience that they have drawn upon? Is there any way for you to test these uncommon beliefs?
6. Reassemble the original group: You should reassemble the original group and have them consider the beliefs that were articulated by them individually in the context of your compliance model, and in the context of how both your company and your industry do business. Lead a discussion that attempts to identify any assumptions or beliefs that "are quite possibly wrong, but worth experimenting with anyway".

7. List of experiments to perform: The authors believe that the outcome of the first six steps will be "a list of possible experiments [tests] to conduct" to determine the validity of the common and uncommon beliefs. These tests can be accomplished in the regular course of business, through a special project with a special team and separate budget. You should agree on the testing process and review your testing assumptions throughout the process. This process can and should take some time so do not set yourself such a tight time frame that it cannot be fully matured.

I find this list to be a very interesting way for a compliance practitioner to get a "tone at the bottom". By engaging employees at the level suggested by the authors, I believe you can find out what the employees think about the company compliance program, and use their collective experience to help design a better and more effective program. It is my belief that employees want to do business in an ethical manner. Giving the chance to engage in business the right way, as opposed to cheating, will win the hearts and minds of your employees almost every time. By using the protocol suggested by the authors, you can not only find out the *effect* of your company's compliance program on the employees at the bottom but you can *affect* it as well.

The bottom line is that a company must both "talk the talk" and "walk the walk" of compliance. Donna Boehme says that it is really about the culture of compliance in your organization. Put another way, as Mike Volkov wrote in an article on his blog, *Corruption, Crime & Compliance*, "Even when a company does all the right things at the senior management level, the real issue is whether or not that culture has embedded itself in middle and lower management. A company's culture is reflected in the values and beliefs that exist throughout the company."[3] You must find a way to articulate and then drive the message of ethical values and doing business in compliance with such anti-corruption laws such as the FCPA from the top down, throughout your organization.

References

1. Bryant, A. "If the Supervisors Respect Values, So Will Everyone Else", *New York Times*, 26 January 2013, see www.nytimes.com/2013/01/27/business/victoria-ransom-of-wildfire-on-instilling-a-companys-values.html?_r=0.
2. Goddard, J., Birkinshaw, J., and Eccles, T., "Uncommon Sense: How to Turn

Distinctive Beliefs Into Action", *MIT Sloan Management Review*, 20 March 2012, see sloanreview.mit.edu/article/uncommon-sense-how-to-turn-distinctive-beliefs-into-action.

3. Volkov, M., "Mood in the Middle Versus Tone at the Top", *Corruption, Crime & Compliance* blog post, 11 March, 2014, see corruptioncrimecompliance.com/2014/03/mood-in-the-middle-versus-tone-at-the-top.

Chapter 2: Some written controls

THE CORNERSTONE of a FCPA compliance program is its written protocols. This includes a code of conduct, policies, and procedures. These requirements have long been memorialized in the US Sentencing Guidelines, which contain seven basic compliance elements that can be tailored to fit the needs and financial realities of any given organization. From these seven compliance elements, the DOJ has crafted its minimum best practices compliance program, which is now attached to every deferred prosecution agreement (DPA) and non-prosecution agreement (NPA). These requirements were incorporated into the 2012 FCPA Guidance. The US Sentencing Guidelines assume that every effective compliance and ethics program begins with a written standard of conduct, i.e. a code of conduct. What should be in this "written standard of conduct"?

Standards of conduct, policies, and procedures (a code of conduct)

> An organization should have an established set of compliance standards and procedures. These standards should not be a "paper only" document, but a "living" document that promotes organizational culture, that encourages "ethical conduct", and that fosters a commitment to compliance with applicable regulations and laws.

In the FCPA Guidance, the DOJ and SEC state, "A company's code of conduct is often the foundation upon which an effective compliance program is built. As

DOJ has repeatedly noted in its charging documents, the most effective codes are clear, concise, and accessible to all employees and to those conducting business on the company's behalf." Indeed, it would be difficult to effectively implement a compliance program if it was not available in the local language so that employees in foreign subsidiaries can access and understand it. When assessing a compliance program, DOJ and SEC will review whether the company chapter has taken steps to make certain that the code of conduct remains current and effective and whether a company has periodically reviewed and updated its code."

In each DPA and NPA over the past 36 months, the DOJ has named the following as item number one for a minimum best practices compliance program: "A Company should develop and promulgate a clearly articulated and visible corporate policy against violations of the FCPA, including its anti-bribery, books and records, and internal controls provisions, and other applicable foreign law counterparts (collectively, the 'anti-corruption laws'), which policy shall be memorialized in a written compliance code."

Stephen Martin and Paul McNulty, partners at Baker and McKenzie, developed one of the best formulations that I have seen of these requirements in what they call the "five elements of an effective compliance program". In this formulation, they posit that your code of conduct, policies, and procedures should be grouped under the general classification of "standards and procedures". They articulate that every company has three levels of standards and controls. First, every company should have a code of conduct, which should, most generally, express its ethical principles. But simply having a code of conduct is not enough so a second step mandates that 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. From the base of a code of conduct and standards and policies, 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.

Code of conduct

In an article in the 2014 edition of the *Complete Compliance and Ethics Manual*, Debbie Troklus, Greg Warner, and Emma Wollschlager Schwartz, state that your company's code of conduct "should demonstrate a complete ethical attitude and your organization's 'system-wide' emphasis on compliance and ethics with all applicable laws and regulations".[1] Your code of conduct must be aimed at all employees and all representatives of the organization, not just those most actively involved in known compliance and ethics issues. From the board of directors to volunteers, the authors believe that "everyone must receive, read, understand, and agree to abide by the standards of the code of conduct". This would also include all "management, vendors, suppliers, and independent contractors, which are frequently overlooked groups."

There are several objectives, identified by the authors, which should be communicated in your code of conduct. Of course, the overriding goal is for all employees to follow what is required of them under the code of conduct. You can help insure this by communicating what is required, providing a process for proper decision-making, and then requiring that all persons subject to the code of conduct put these standards into everyday business practice. Such actions are some of your best evidence that your company "upholds and supports proper compliance conduct".

The substance of your code of conduct should be tailored to the company's culture, and to its industry and corporate identity. It should provide a mechanism by which employees who are trying to "do the right thing" in the compliance and business ethics arena can do so. The code of conduct can be used as a basis for employee review and evaluation. It should certainly be invoked if there is a violation. To that end, I suggest that your company's disciplinary procedures be stated in the code of conduct. These would include all forms of disciplinary action, up to and including dismissal, for serious violations of the code of conduct. Further, your company's code of conduct should emphasize that the company will comply with all applicable laws and regulations, wherever it does business. The code needs to be written in plain English and translated into other languages as necessary so that all applicable persons can understand it.

As I often say, the three most important things about your FCPA compliance program are "document, document, and document". The same is true of communicating your company's code of conduct. You need to do more than simply put it on your website and tell folks it is there, available, and that they

should read it. You need to document that all employees, or anyone else that your code of conduct is applicable to, has received, read, and understands it. For employees, it is important that a representative of the compliance department, or other qualified trainer, explains the standards set forth in your code of conduct and answers any questions that an employee may have. Your company's employees need to attest in writing that they have received, read, and understood the code of conduct and this attestation must be retained and updated as appropriate.

The DOJ expects each company to begin its compliance program with a very public and very robust code of conduct. If your company does not have one, you need to implement one forthwith. If your company has not reviewed or assessed their code of conduct for five years, I would suggest that you do so in short order as much has changed in the compliance world in recent years.

What is the value of a code of conduct? I have heard many business folks ask that question over the years. In its early days, a code of conduct tended to be lawyer-written and lawyer-driven, and designed to "wave in a defense situation" so that the company could claim "see we have one". But does such a legalistic code still serve a purpose? Should a code of conduct be more than simply your company's "law"? What is it that makes a code of conduct effective? What should be your goal in creating one for your company?

Carol Switzer, president of the Open Compliance and Ethics Group (OCEG), explored some of these questions in an article in *Compliance Week* in which she interviewed Jimmy Lin, vice president (VP) of product management and corporate development at The Network, and Kendall Tieck, VP of internal audit at Workday, for their thoughts on what makes an effective code of conduct.[2]

Tieck views a code of conduct as not simply a static piece of paper or document "but as a set of expected behaviors that are integral to the fabric of the business and an organization's value system. A code of conduct is not a compliance activity, but how an entity demonstrates integrity and acquires trust from markets, shareholders, customers, partners, and governments. To achieve these outcomes, a careful plan, aligned with a policy lifecycle management framework, should articulate how the Code is integrated in the core of the company's activities and culture."

Switzer believes that one of the key components of a best practices code of conduct is to integrate the connection between a business's objectives, its risk, and its compliance management. There are numerous factors, which can

move a company towards having such an effective integration. Switzer wrote that some of these include, "external stakeholder expectations and pressures, internal culture and context, objectives for the code, process of development and implementation, content of the code, consequences for non-conforming conduct, strength of sub-codes (e.g. policies), and employee character."

Switzer ends her piece by relating that there is a huge benefit to a company for a well-thought-out code of conduct, as a tool to drive both corporate values and sinew the expectations of conduct into the fabric of the company. By designing a code of conduct that can be measured for effectiveness, you can continuously keep the goals moving. Switzer laid out six steps for the compliance practitioner to think through and implement during a code of conduct upgrade or rewrite. These six steps are:

1. Design;
2. Deliver;
3. Interact;
4. Measure;
5. Maintain; and
6. Improve.

Design

Under this step, a company needs to define the behavior that it desires to inspire and allow employees to collaborate at all levels. Lin said that a key aspect was relevancy, "But times change—business environments change, cultures change, risk appetites change. We all need to keep in mind that the Code, the ultimate policy, should not be a stale document on the shelf. It needs to inspire, engage, and change with the organization." Tieck said that your code of conduct should be "considered a part of the entity's overall policy landscape. Leveraging an effective policy lifecycle management framework will promote integration and alignment across the policy governance landscape."

Deliver

Switzer also identified the delivery of a code of conduct as a key element in its effectiveness. She said, "modern communication methods that allow the user to engage, interact, and research further behind the Code into related policies, procedures, and helplines for additional guidance can be better monitored and measured. Code content that is integrated with efforts to monitor changes in

the external and internal environment can be updated as needed rather than on a static schedule." This should also include relevant third parties such as suppliers and sales agents. "And failure to comply with the Code can be better identified and tracked, indicating possible need for clarification, additional training, or better screening of employees."

Interact

Lin pointed out that a code of conduct is both a corporate governance document and a marketing document. As such, you will need to create a marketing campaign to get the message out to your employee base, and to relevant third parties. If you have a large number of non-English speaking personnel or employees without access to online training, these factors need to be considered when determining the delivery method.

Measure

Initially, you should prioritize both qualitative results and positive feedback by including such metrics as speed of completion, reminders to be sent to facilitate completion of code of conduct training, and the percentage of employees and third parties who attest to the review of your code of conduct. You should also measure the effectiveness of your communication campaign. Tieck suggests drilling down further because each component of your code of conduct sets "an expected behavior. Selecting a few critical behaviors to measure and monitor may be adequate for most organizations. These selected measures might represent an aggregate measure of the overall conformance to the code. Large organizations may be able to mine HR data to capture statistics associated with the identified behaviors. For instance, termination reason codes may be one source."

Maintain

All commentators note that it is important to keep your code of conduct design and content fresh. One way to do so is by using employee feedback to identify whether your code of conduct is not only *effective*, but also truly *reflective* of your company's culture. Lin points out that to gain these insights you need to incorporate both formal and informal techniques for gauging the relevant employee and third party populations. He states, "Questionnaires, surveys, forms and hotlines can be good anonymous sources, but engaging employees in conversation is just as, if not more, important. Make sure

executives and managers alike spend time in small-group and one-on-one conversations. Have these conversations throughout the year and across your employee base to get the 'real' story. This helps engage the employees and ensure they know you value their input."

Improve

OCEG advocates that your code of conduct should be evaluated for revision at least every two years. This should be done to keep abreast of the changes in laws and regulations and your own business operations and risk tolerances. Switzer says, "Code content that is integrated with efforts to monitor changes in the external and internal environment can be updated as needed rather than on a static schedule."

Policies, procedures, and controls

The written policies and procedures required for a best practices compliance program are well known and long established. As stated in the FCPA Guidance, "Among the risks that a company may need to address include the nature and extent of transactions with foreign governments, including payments to foreign officials; use of third parties; gifts, travel, and entertainment expenses; charitable and political donations; and facilitating and expediting payments." Policies help form the basis of expectation and conduct in your company, and procedures are the documents that implement these standards of conduct.

Another way to think of policies, procedures, and controls was stated by Aaron Murphy, now a partner at Aiken Gump, in his book *Foreign Corrupt Practices Act*, when he said that you should think of all three as "an interrelated set of compliance mechanisms".[3] Murphy went on to say that, "Internal controls are policies, procedures, monitoring and training that are designed to ensure that company assets are used properly, with proper approval and that transactions are properly recorded in the books and records. While it is theoretically possible to have good controls but bad books and records (and vice versa), the two generally go hand in hand – where there are record-keeping violations, an internal controls failure is almost presumed because the records would have been accurate had the controls been adequate."

Borrowing from an article in the *Houston Business Journal* by John Allen,[4] I found some interesting and important insights into the role of policies in any anti-corruption compliance program. Allen says that the role of policies is "to protect companies, their employees and consumers, and despite an occasional

opposite outcome, that is typically what they do. A company's policies provide a basic set of guidelines for their employees to follow. They can include general dos and don'ts or more specific safety procedures, work process flows, communication guidelines or dress codes. By establishing what is and isn't acceptable workplace behavior, a company helps mitigate the risks posed by employees who, if left unchecked, might behave badly or make foolhardy decisions."

Allen notes that policies "are not a surefire guarantee that things won't go wrong, they are the first line of defense if things do". The effective implementation and enforcement of policies demonstrates to regulators and the government that a "company is operating professionally and proactively for the benefit of its stakeholders, its employees and the community it serves". If it is a company subject to the FCPA, by definition, it is an international company so that can be quite a wide community.

Allen believes that there are five key elements to any "well-constructed policy". They are:

1. Identify to whom the policy applies;
2. Establish the objective of the policy;
3. Explain why the policy is necessary;
4. Outline examples of acceptable and unacceptable behavior under the policy; and
5. Warn of the consequences if an employee fails to comply with the policy.

Allen notes that, for polices to be effective, there must be communication. He believes that training is only one type of communication. I think that this is a key element for compliance practitioners, because if you have a 30,000 plus worldwide work force, the logistics alone of such training can appear daunting. Small groups, where detailed questions about policies can be raised and discussed, can be a powerful teaching tool. Allen even suggests posting FAQs in common areas as another technique. It is worth noting that one of the reasons Morgan Stanley received a declination to prosecute by the DOJ was that it sent out bi-monthly compliance reminder emails to its employee Garth Peterson for the seven years he was employed by the company.

The FCPA Guidance ends its section on policies with the following statement, "Regardless of the specific policies and procedures implemented, these

standards should apply to personnel at all levels of the company." Allen puts a bit differently: "it is important that policies are applied fairly and consistently across the organization". He notes that where policies are applied inconsistently, "there is a greater chance that an employee dismissed for breaching a policy could successfully claim he or she was unfairly terminated". This last point cannot be over-emphasized. If an employee is going to be terminated for fudging their expense accounts in Brazil, you had best make sure that same conduct lands your top producer in the US with the same quality of discipline.

Revising your code of conduct, policies, and procedures

Simply having a code of conduct, together with compliance policies and procedures, is not enough. As articulated by former assistant attorney general for the Criminal Division of the DOJ, Lanny Breuer, "Your compliance program is a living entity; it should be constantly evolving." This was echoed in an article in the SCCE magazine in which authors Anne Marie Logarta and Ruth Ward suggest considering the following issues before you take on an update of your code of conduct:[5]

- When was the last time your code of conduct was released or revised?
- Have there been changes to your company's internal policies since the last revision?
- Have there been changes to relevant laws relating to a topic covered in your company's code of conduct?
- Are any of the guidelines outdated?
- Is there a budget to create/revise a code?

After considering these issues, the authors suggest that you should benchmark your current code of conduct against that of other companies in your industry. I would also add that your standards, policies, and procedures should be reviewed and updated in the same manner. If you decide to move forward, the authors have a six-point guide, which they believe will assist you in making your revision process successful. I have used this as a basis from which to set out a plan for revisions to your compliance policies and procedures.

1. Get buy-in from decision makers at the highest level of the company

The authors believe that your company's highest level must give the mandate

for a revision to a code of conduct and compliance policies and procedures. It should be for the CEO, GC, or CCO (or better yet all three) to mandate this effort. Whoever gives the mandate, this person should be "consulted at every major step of the Code review process if it involves a change in the direction of key policies".

2. Establish a core revision committee

A cross-functional working group would be ideal to head up your effort to revise your code of conduct and compliance policies and procedures. This group should include representatives from the following departments: legal, compliance, communications, and HR. There should also be other functions, which represent the company's domestic and international business units; finally, there should be functions within the company represented, such as finance and accounting, IT, marketing, and sales.

From this large group, the topics can be assigned for initial drafting to functions based on "relevancy or necessity". These different functions would also solicit feedback from their functional peers and deliver a final, proposed draft to the drafting committee. The authors emphasize that creation of a "timeline at the outset of the revision is critical and [you should] hold the function representatives accountable for meeting their deliverables".

3. Conduct a thorough technology assessment

The cornerstone of the revision process is how your company captures, collaborates, and preserves "all of the comments, notes, edits, and decisions during the entire project". Here technology such as SharePoint or Google Cloud can be of great assistance to accomplish this process, even if you are required to train team members on their use. In addition to using technology to draft your code of conduct and compliance policies and procedures revisions, you should determine if these will be available in hard copy, online, or both. If it will be available online, you should assess "the best application to launch your Code and whether it includes a certification process". Lastly, there must be a distribution plan, particularly if the code and compliance policies and procedures will only be available in hard copy.

4. Determine translations and localizations

The authors emphasize, "If your company does business internationally, then

this step is vital to ensure you have one Code, no matter the language." They also note that if you decide to translate your code of conduct, you should be sure to hire someone who is an "approved company translation subject matter expert".[6] The essential is that "your employees have the same understanding of the company's Code – no matter the language".

5. Develop a plan to communicate the code of conduct

Rollout is always critical because it "is important that the new or revised Code is communicated in a manner that encourages employees to review and use the Code on an ongoing basis". Your company should use the full panoply of tools available to it to publicize your new or revised code of conduct and compliance policies and procedures. This can include a multi-media approach or physically handing out a copy to all employees at a designated time. You might consider having a company-wide code of conduct and compliance policies and procedures meeting where the new or revised documents are rolled out across the company all in one day. And remember, with all things compliance, the three most important steps are "document, document, and document"! However you deliver the new or revised code of conduct, you must document that each employee has received it.

6. Stay on target

The authors end by noting that, if you set realistic expectations, you should be able to stay on deadline and stay within your budget. They recommend that you "set aside enough time so that you won't feel rushed or in a hurry to get it done". They also reiterate that it is essential to keep a close watch on your budget so that you do not exceed it. These points are a useful guide to not only thinking through how to determine if your code of conduct, and compliance policies and procedures needs updating, but also practical steps on how to tackle the problem when it arises. It is far better to review and update as appropriate than to wait for a massive FCPA investigation to go through the process.

There are numerous reasons to put some serious work into your code of conduct, policies, and procedures. They are certainly a first line of defense when the government comes knocking. The FCPA Guidance makes clear that "Whether a company has policies and procedures that outline responsibilities for compliance within the company, detail proper internal controls, auditing practices, and documentation policies, and set forth disciplinary procedures

will also be considered by DOJ and SEC [emphasis added]." By "considered", I think it is clear that this means the regulators will take a strong view against a company that does not have well-thought-out and articulated policies, procedures, and a code of conduct, all of which are systematically reviewed and updated. Moreover, as emphasized by Allen, "having policies written out and signed by employees provides what some consider the most vital layer of communication". Together with a signed acknowledgement, these documents can serve as evidentiary support if a future issue arises. In other words, the "document, document, and document" mantra applies just as strongly to this area of anti-corruption compliance.

References

1. Troklus, D., Warner, G., and Wollschlager Schwartz, E., "Essential Elements of an Effective Ethics and Compliance Program", in the *Society for Corporate Compliance and Ethics (SCCE) Complete Compliance and Ethics Manual* – 2014 (2nd edition).
2. Switzer, C., "The code of conduct Conundrum", *Compliance Week*, 31 December 2014, see www.complianceweek.com/news/news-bulletin/the-code-of-conduct-conundrum.
3. Murphy, A. G., *Foreign Corrupt Practices Act*, Hoboken, NJ: Wiley, January 2011.
4. Allen, J., "Company policies are source and structure of stability", *Houston Business Journal*, 12 June 2013, see www.bizjournals.com/bizjournals/how-to/human-resources/2013/07/company-policies-are-source-of.html?page=all.
5. Logarta, A.M., and Ward, R., "Six steps for revising your company's code of conduct", *Compliance & Ethics Professional*, July/August 2012, see www.sccemagazine.org/complianceandethicsprofessional/20120708?pg=46#pg46.
6. Personally, I would recommend contacting Jay Rosen at Merrill Brink, which is one of the top language service providers.

Chapter 3: For the CCO – Oversight, autonomy, and resources

Autonomy

There is an ongoing debate in the compliance world about whether a company can or should combine or separate the role of the CCO from that of the GC. However, before a company can answer this question, it must meet requirement six of the DOJ minimum best practices requirements for a FCPA-based compliance program, which reads:

"The company will assign responsibility to one or more senior corporate executives for the implementation and oversight of the company's anti-corruption policies, standards, and procedures. Such corporate official(s) shall have direct reporting obligations to independent monitoring bodies, including internal audit, Company's board of directors, or any appropriate committee of the board of directors, and shall have an adequate level of autonomy from management as well as sufficient resources and authority to maintain such autonomy."

The 2011 Amendments to the US Sentencing Guidelines, section 8B2.1 (b)(2)(C), specified: "Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority."

There has traditionally been divided opinion in companies as to whether the CCO should report into a legal function and the GC, or report directly to a company's head officer. Mike Volkov noted that, "According to the last

PWC Compliance Survey, only 29 per cent of CCOs have made it into the C-Suite but that will increase. Only 27 per cent of CCOs continue to report to the general counsel while 34 per cent report directly to the CEO."[1] Whichever path your company employs, it is imperative that the CCO speak from a position of authority.

Noted compliance expert Donna Boehme writes and speaks consistently on the characteristics necessary for a successful CCO. Writing in the SCCE magazine, *Compliance & Ethics Professional*, Boehme articulated five essential features required for a CCO to be successful in an organization.[2] These are outlined below.

1. Independence

It is incumbent on any CCO to have "sufficient authority and independence to oversee the integrity of the compliance program".[3] Some indicia of independence would include a reporting line to the company's board of directors and audit/compliance committee, and more importantly "unfiltered" access to the board. There should also be protection of employment, including an employment contract with a "nondiscretionary escalation clause" and a requirement for board approval for any change in the terms and conditions of employment, including termination. There must also be sufficient resources in the form of an independent budget and adequate staff to manage the overall compliance program.

2. Empowerment

A CCO must have "the appropriate unambiguous mandate, delegation of authority, senior-level positioning, and empowerment to carry out his/her duties. Such can be accomplished through a "board resolution and a compliance charter, adopted by the board". Additionally, the CCO job description should be another manner in which to clarify the CCO "mandate, and at a minimum should encompass the single point accountability to develop, implement and oversee an effective compliance program". All of the above should lead in practice to a "close working relationship with an independent board committee".

3. Seat at the table

The CCO must "have formal and informal connections into the business and functions of the organization – a seat at the table at important meetings where all major business matters (e.g., risk, major transactions, business

plans) are discussed and decided". She argues that, at a minimum, the CCO should participate in "budget reviews, strategic planning meetings, disclosure committee meetings, operational reviews, and risk and crisis management meetings".

4. Line of sight

The CCO should have "unfettered access to relevant information to be able to form independent opinions and manage the [compliance] program effectively". This does not mean that the CCO should have veto power over functions such as safety or environmental, or that such functions must report to the CCO, but unless there is visibility to the CCO for these risk areas, the CCO will not be able to adequately assess and manage such risks from the compliance perspective. The correct structuring of the CCO role to allow it access to and visibility in these areas will help the CCO to coordinate compliance convergence training.

5. Resources

It is absolutely mandatory that the CCO be given the physical resources, in terms of personnel and monetary resources, to "get the job done". I have worked at places where the CCO had neither, and the CCOs did not succeed because they never even had the chance to do so. Boehme focuses on both types of resources. Under monetary resources, she points as an indication to the independence of the CCO from the general counsel "rather than a shared budget". This can also bleed over to "headcount" and shared or dotted line reporting resources. There should be independent resources reporting into the compliance function.

The board

FCPA Guidance and US Sentencing Guidelines

A board's duty under the FCPA is well known. In the FCPA Guidance, there are two specific references to the obligations of a board within the "hallmarks" of an effective compliance program. The first hallmark states, "Within a business organization, compliance begins with the board of directors and senior executives setting the proper tone for the rest of the company". The second reference is found under hallmark number three, entitled "Oversight, Autonomy and Resources", which suggests that the CCO should have "direct access to an organization's governing authority, such as the board of directors and

committees of the board of directors (e.g., the audit committee)". Further, under the US Sentencing Guidelines, the board must exercise reasonable oversight on the effectiveness of a company's compliance program. The DOJ's Prosecution Standards posed the following queries:

1. Do the directors exercise independent review of a company's compliance program? and
2. Are directors provided with sufficient information to enable the exercise of independent judgment?

Board failure to heed this warning can lead to serious consequences. David Stuart, an attorney with Cravath, Swaine & Moore LLP, noted that FCPA compliance issues can lead to personal liability for directors, as both the SEC and DOJ have been "very vocal about their interest in identifying the highest-level individuals within the organization who are responsible for the tone, culture, or weak internal controls that may contribute to, or at least fail to prevent, bribery and corruption". He added that, based upon the SEC's enforcement action against two senior executives at Nature's Sunshine Products, "Under certain circumstances, I could see the SEC invoking the same provisions against audit committee members—for instance, for failing to oversee implementation of a compliance program to mitigate risk of bribery". It would not be too much of a leap from here for the SEC to next invoke the same provisions against audit committee members who do not actively exercise oversight of an ongoing compliance program.

There is one other issue regarding the board and risk management, including FCPA risk management, which should be noted. It appears that the SEC desires boards to take a more active role in overseeing the management of risk within a company. The SEC has promulgated Regulation SK 407 under which each company must make a disclosure regarding the board's role in risk oversight, which "may enable investors to better evaluate whether the board is exercising appropriate oversight of risk". If this disclosure is not made, it could be a securities law violation and subject the company that fails to make it to fines, penalties, or profit disgorgement.

I believe that a board must not only have a corporate compliance program in place but actively oversee that function. Further, if a company's business plan includes a high-risk proposition, there should be additional oversight. In other words, there is an affirmative duty to ask the tough questions. But it is more

than simply having a compliance program in place. The board must exercise appropriate oversight of the compliance program and indeed the compliance function. The board needs to ask the hard questions and be fully informed of the company's overall compliance strategy going forward.

Boards of directors and compliance: Four areas of inquiry

One approach a board could take was articulated by Amy Hutchens, president and founder at CLEAResources, LLC.[4] Hutchens' guidance was centered on four core areas upon which directors should focus their attention:

1. Structure;
2. Culture;
3. Areas of risk; and
4. Forecasts.

Structure questions

This area consists of questions which will aid in determining the fundamental sense of a company's overall compliance program. The questions should begin with the basics of the program through to how the program operates in action. These inquiries should allow each board member to understand the main elements of a compliance program. Using Hutchens' guidance as a starting point, here are some structure questions board members might ask.

- Who oversees the operation of the compliance program?
- What is in the code of conduct? Is each board member aware of corporate standards and procedures?
- How are complaints about violation of the company's compliance program being received?
- Who conducts investigations and takes action on the results?
- What corporate resources are being devoted to the compliance program?
- How much money is allocated to the program?
- What types of training are required? How effective are they?
- Have any compliance failures been detected? If so, how was such detection made?
- If a company's compliance program is less mature, what are the charter compliance documents?
- If a company's compliance program is more mature, there should be

queries regarding the roles of the general counsel vs. a chief compliance officer. If a CCO is required, where would such a person sit in the organization, and what is the CCO reporting structure?

Culture questions

This area of inquiry should focus on the culture of the organization as it concerns compliance. Board members should have an understanding of what message is being communicated, not only from senior management but also middle management. Equally important, the board needs to understand what message is being heard at the lowest levels within the company. Hutchens suggests that board members ask some of the following culture questions:

- When did the company last conduct a survey to measure the corporate culture of compliance?
- Is it time for the company to resurvey to measure the corporate culture of compliance?
- If a survey is performed, what are the results? Have any deficiencies been demonstrated? If so, what is the action plan going forward to remedy such deficiencies?
- Did any compliance investigations arise from a cultural problem?
- Regardless of any survey results, what can be done to improve the culture of compliance within the company?
- If there were any acquisitions, were they analyzed from a compliance culture perspective?
- Are there any M&A deals on the horizon, have they been reviewed from the compliance perspective?

Areas of risk

Here Hutchens recommends that board members "need to know what process is being used to identify emerging risks". Such risk analysis would be broader than simply a legal/compliance risk assessment and should be tied to other matters, such as "business continuity planning and crisis response plans".

Noting that "the board of directors needs to use their expertise and ask the right questions", Hutchens gave the following examples:

- What is the risk assessment process?
- How effective is this risk assessment process? Is it stale?
- Who is involved in the risk assessment process?

- Does the risk assessment process take into account any new legal or compliance best practices developments?
- Are there any new operations that pose substantial compliance risks for the company?
- Is the company tracking enforcement trends? Are any competitors facing enforcement actions?
- Has the company moved into any new markets which impose new or additional compliance risks?
- Has the company developed any new product or service lines which change the company's risk profile?

Forecast

Hutchens believes that "a truly effective and informed board knows where the company stands not only at the present moment, but also has the strategic plan for how the compliance and ethics program can continue to grow". However, a compliance program should be nimble enough to respond to new information or actions, such as mergers or acquisitions, divestitures, or other external events. If a dynamic changes, "you want to get your board's attention on the changes which may need to happen with the [compliance] program". Hutchens believes that such agility is best accomplished by obtaining buy-in from the board by ensure that they understand the role of forecasting the compliance program going forward.

20 questions directors should ask about compliance committees

Another approach is presented through the following list of 20 questions reflecting the oversight role of directors, which was provided to me by Stephen Martin who currently runs Baker & McKenzie Compliance Consulting, LLC. The questions are not intended to be an exact checklist, but rather a way to provide insight and stimulate discussion on the topic of compliance. The questions provide directors with a basis for critically assessing the answers they get and digging deeper as necessary. Although the questions apply to most medium to large organizations, the answers will vary according to the size, complexity, and sophistication of each individual organization.

Part I: Understanding the role and value of the compliance committee

1. What are the compliance committee's responsibilities and what value does it bring to the board?

2. How can the compliance committee help the board enhance its relationship with management?
3. What is the role of the compliance committee?

Part II: Building an effective compliance committee

4. What skill sets does the compliance committee require?
5. Who should sit on the compliance committee?
6. Who should chair the compliance committee?

Part III: Directed to the board

7. What is the compliance committee's role in building an effective compliance program within the company?
8. How can the compliance committee assess potential members and senior leaders of the company's compliance program?
9. How long should directors serve on the compliance committee?
10. How can the compliance committee assist directors in retiring from the board?

Part IV: Enhancing the board's performance effectiveness

11. How can the compliance committee assist in director development?
12. How can the compliance committee help the board chair sharpen the board's overall performance focus?
13. What is the compliance committee's role in board evaluation and feedback?
14. What should the compliance committee do if a director is not performing or not interacting effectively with other directors?
15. Should the compliance committee have a role in chair succession?
16. How can the compliance committee help the board keep its mandates, policies, and practices up to date?

Part V: Merging roles of the compliance committees

17. How can the compliance committee enhance the board's relationship with institutional shareholders and other stakeholders?
18. What is the compliance committee's role in CCO succession?
19. What role can the compliance committee play in preparing for a crisis, such as discovering of a sign of a significant compliance violation?
20. How can the compliance committee help the board in deciding CCO pay and bonus?

Whichever approach that you employ, whether the 20 questions or the four-part approach suggested by Hutchens or another approach, you need to lay out a clear and logical program for a board of directors to not only understand its role in the compliance function, but to play an active role in this. Any best practices compliance program has several moving parts: a CCO to lead the compliance program, a compliance department to execute the strategy, and an engaged board of directors who oversee and participate.

More than simply asking questions, it is important that the CCO share information with rest of management in advance of the board meeting, creating transparency. As the CCO works with the general counsel, outside legal counsel, and outside external audit quite closely throughout the year, they must continue to work with them closely during the preparation of the annual compliance report. Lastly, and from my experience always the most important aspect of any relationship with senior management or the board, make sure there are *no surprises*.

Resources

Funding the compliance program is always one of the biggest challenges for any CCO. Short of being in the middle of a worldwide FCPA, UK Bribery Act, or other anti-corruption investigation, you are never going to receive all the funding you want or even think that you are going to need. But this corporate reality is not going to save you if the government comes knocking. The FCPA Guidance provides the following, "…the amount of resources devoted to compliance will depend on the company's size, complexity, industry, geographical reach, and risks associated with the business. In assessing whether a company has reasonable internal controls, DOJ and SEC typically consider whether the company devoted adequate staffing and resources to the compliance program given the size, structure, and risk profile of the business."

Former DOJ prosecutor Stephen Martin often describes an inquiry he might have made in this position, which goes along the lines of the following. First, he would ask someone who came in before the DOJ what the company's annual compliance budget was for the past year. If the answer started with something like, "We did all we could with what we had ($100K, $200K, name the figure), he would then ask, "How much was the corporate budget for post-it notes last year?" The answer was always in the seven-figure range. His next question would then be, "Which is more business critical for your company; complying with the FCPA or post-it notes?" Unfortunately, it has been

Martin's experience that most companies spent far more on the post-it notes than they were willing to invest into their compliance program.

However, there are some things that a CCO might do to try to obtain the resources needed. One thing you can do is have a list of information prepared and be ready to present to the board or CEO who may provide funding for your compliance function. If you lay out the information in a coherent manner, it would allow the board or senior management to get some perspective on the compliance function: what you are asking for and why. The presentation might include:

- Executive summary: This should be no more than three pages and it should convey excitement and impact. It must spell out your compliance mission and clearly state the opportunities that are presented for your compliance group to not only further the goals of compliance with the FCPA or UK Bribery Act, but also how these opportunities will result in increased earnings and profits.
- The industry: Here is an opportunity for benchmarking within your industry. You should use credible research from recognized authorities or collect the information from your counterparts in other companies directly, if such information is available to you. You should focus on the size, growth, and significance of compliance within your industry and the opportunities for growth within your company.
- The company: Here you should walk the reader through how your compliance program has grown; this could include organic growth, detailing areas that you may have engaged in as best practices have evolved, and growth of your compliance regime through acquisitions. You should also share major victories and tie all of these into your company values as set out in your published code of conduct.
- Management and ownership: Here is an opportunity for you to recognize the persons in your compliance organization. You should have an organizational chart, biographies of key personnel, and anticipated hiring needs.
- Financial information/projections: Here you should create a three-year forecast using best, probable, and worst-case scenarios for each year on a cash basis. In this section, you should include historical return on investment (ROI) figures from prior initiatives, to the extent that you have any, and end with a current balance sheet that will indicate and extend top and bottom-line growth for your compliance department.

- Purpose of the investment: Here you need to be short, compelling, and to the point. You should spell out precisely what you are asking for and reiterate what you will do with the funding.

Once again, recognizing that every compliance function will always be resource constrained, you can look to other areas in your company to assist the compliance function. An obvious starting place is human resources (HR). There are several areas in which HR can bring expertise and, in my experience, enthusiasm to the compliance function. Some of the reasons include the fact that HR is physically located at or touches every site in the company, globally. HR is generally seen as more approachable than many other organizations within a company, unfortunately this includes compliance.
A person's first touch point with a company is often HR in the interview process. If not in the interview process, it is certainly true after a hire is made. Use this approachability.

HR has several key areas of expertise, such as in discrimination and harassment. But beyond this expertise, HR also has direct accountability for these areas. It does not take a very long or large step to expand this expertise into assistance for compliance. HR is often on the front line for hotline intake and responses. These initial responses may include triage of the complaint and investigations. With some additional training, you can create a supplemental investigation team for the compliance department.

Clearly, part of HR's role is to run or organize training. By "training the trainers" on compliance, you may well create an additional training force for your compliance department. HR can also give compliance advice on the style and tone of training. The things that might work and even be legally mandated in Texas may not work in other areas of the globe; advice can be of great assistance. But more than just putting on the training, HR often maintains employee records of training certifications, certifications to your company's code of conduct, and compliance requirements. This can be the document repository for the "document, document, and document" portion of your compliance program.

Internal audit is another function that you may want to look to for assistance. Obviously, internal audit should have access to your company's accounting systems. This can enable them to pull data for ongoing monitoring. This may allow you to move toward continuous controls monitoring on an internal basis. Similarly, one of the areas of core

competency of internal audit should also be internal controls. You can have internal audit assist in a gap analysis to understand what internal controls your company might be missing.

As this corporate function's name implies, internal audit routinely performs internal audits of a company. You can use this routine job duty to assist compliance. There will be an existing audit schedule and you can provide some standard compliance issues to be included on each audit. Further, compliance risks can also be evaluated in this process. Similar to the audit function are investigations. With some additional training, internal audit should be able to assist the compliance function to carry out or participate in internal compliance investigations. Lastly, internal audit should be able to assist the compliance function to improve controls following investigations.

A corporate IT department has several resources that can also assist compliance, including IT controls, IT equipment, and access to data. This can help you to facilitate investigations by giving you (1) access to email and (2) access to databases within the company. Similar to the above functions, IT will also be a policy owner so you can turn to them for any of your compliance program requirements which may need a policy that touches on their areas of expertise. The final consideration for IT assistance is in the area of internal corporate communication. IT enables communications within a company. You can use IT to aid in your internal company intranet, online training, newsletters, or the often-mentioned "compliance reminders".

Finally, do not forget your business teams. You can embed a compliance champion in all divisions and functions around the company. You can take this a step further by placing a facility compliance officer at every site or location where you might have a large facility or corporate presence. Such local assets can provide feedback for new policies to let you know if they do not they make sense. In some new environments, a policy may not work. If you company uses SAP and you make an acquisition of an entity which does not use this enterprise resource planning (ERP) system, your internal policy may need to be modified or amended. A business unit asset can also help to provide a push for training and communications to others who are similarly situated. One thing that local compliance champions can assist with is helping to set up and coordinate personnel for interviewing employees. This is an often over-looked function, but local coordination is always easier than from the corporate office.

References

1. Volkov, M., "The CCO's Challenge: Becoming a Strategic Business Partner", *Corruption, Crime & Compliance* blog post, 23 July 2014, see corruptioncrimecompliance.com/2014/07/the-ccos-challenge-becoming-a-strategic-business-partner.
2. Boehme, D., "Five essential features of the Chief Ethics and Compliance Officer position", *Compliance Today*, December 2012.
3. Ibid.
4. Jaeger, J., "Board Checklist: What Every Director Should Know", *Compliance Week*, 1 November 2011, see www.complianceweek.com/news/news-bulletin/board-checklist-what-every-director-should-know.

Chapter 4: The cornerstone of your compliance program – Risk assessments

ONE CANNOT really say enough about risk assessments in the context of anti-corruption programs. Since at least 1999, in the *Metcalf & Eddy* enforcement action,[1] the DOJ has said that risk assessments that measure the likelihood and severity of possible FCPA violations should also identify how you should direct your resources to manage these risks. The FCPA Guidance stated it succinctly when it said, "Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company's compliance program." The UK Bribery Act takes a similar view; in principle three of the six principles of an adequate compliance program (part of the Guidance to the Act), it states, "The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. This assessment is periodic, informed and documented." In other words, risk assessments have been around and even mandated for a long time and their use has not lessened in importance. The British have a way with words, even when discussing compliance, and principle one of the six principles says that your risk assessment should *inform* your compliance program.

Jonathan Marks, a partner in the firm of Crowe Horwath LLP, said the following about risk assessments in his 13-step "FCPA compliance action plan", "A comprehensive assessment of the potential bribery and corruption risks – both existing and emerging risks – associated with a company's products and services, customers, third-party business partners, and geographic locations can serve as the basis for the compliance program. The risk assessment determines the areas at greatest risk for FCPA violations among all types of international business transactions and operations, the business culture of each country in which these activities occur, and the integrity and reputation of third parties engaged on behalf of the company."

The simple reason is straightforward: you cannot define, plan for, or design an effective compliance program to prevent bribery and corruption unless you can measure the risks you face. Both the US Sentencing Guidelines and the UK Bribery Act's Guidance place emphasis on risk assessment in their respective recommendations for creating an effective anti-corruption and anti-bribery program.

What should you assess?

In 2011, the DOJ concluded three FCPA enforcement actions, which specified factors a company should review when making a risk assessment. The three enforcement actions, involving the companies Alcatel-Lucent SA, Maxwell Technologies Inc., and Tyson Foods Inc. all had common areas that the DOJ indicated were FCPA compliance risk areas, which should be evaluated for a minimum best practices FCPA compliance program. Both the Alcatel-Lucent and Maxwell Technologies Deferred Prosecution Agreements (DPAs) listed the seven following areas of risk to be assessed.

1. Geography: Where the company does business;
2. Interaction with types and levels of governments;
3. Industrial sector of operations;
4. Involvement with joint ventures;
5. Licenses and permits in operations;
6. Degree of government oversight; and
7. Volume and importance of goods and personnel going through customs and immigration.

All of these factors were reiterated in the FCPA Guidance which stated, "Factors to consider, for instance, include risks presented by: the country and industry sector, the business opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs."

These factors provide guidance into some of the key areas that the DOJ apparently believes can put a company at higher FCPA risk. These factors supplement those listed in the UK Bribery Act Guidance, which points to several key risks which should be evaluated in this process. These risk areas include:

1. Internal risk. This could include deficiencies in:

    i. Employee knowledge of a company's business profile and understanding of associated bribery and corruption risks;
    ii. Employee training or skills sets; and
    iii. The company's compensation structure or lack of clarity in the policy on gifts, entertaining, and travel expenses.

2. Country risk. This type of risk could include:

    i. Perceived high levels of corruption as highlighted by corruption league tables published by reputable Non-Governmental Organizations (NGOs), such as Transparency International;
    ii. Factors such as absence of anti-bribery legislation; lack of implementation; or a perceived lack of government capacity or media, local business community, or civil society influence in effectively promoting transparent procurement and investment policies; and
    iii. A culture which does not punish those who seek bribes or make other extortion attempts.

3. Transaction risk. This could include, for example, transactions involving charitable or political contributions, the obtaining of licenses and permits, public procurement, high value or projects with many contractors, or involvement of intermediaries or agents.

4. Partnership risks. This risk could include foreign business partners located in higher-risk jurisdictions, associations with prominent public office holders, and insufficient knowledge or transparency of third party processes and controls.

Another approach was detailed by David Lawler in his book *Frequently Asked Questions in Anti-Bribery and Corruption*. He broke the risk areas to evaluate down into the following categories: (1) company risk; (2) country risk; (3) sector risk; (4) transaction risk; and (5) business partnership risk. He further detailed these categories as follows:

1. Company risk. Lawler believes this is "only to be likely to be relevant when assessing a number of different companies – either when managing a portfolio

of companies from the perspective of a head office of a conglomerate or private equity house." High-risk companies involve some of the following characteristics:

i. Private companies with a close shareholder group;
ii. Large, diverse, and complex groups with a decentralized management structure;
iii. An autocratic top management;
iv. A previous history of compliance issues; and/or
v. Poor marketplace perception.

2. Country risk. This area involves countries that have a high reported level or perception of corruption, have failed to enact effective anti-corruption legislation, and have failed to be transparent in their procurement and investment policies. Obviously, the most recent Transparency International Corruption Perceptions Index is a good starting point. Other indices you might consider are the Worldwide Governance Indicators and the Global Integrity Index.

3. Sector risk. This involves areas which require a significant amount of government licensing or permissions to do business in a country. It includes the usual suspects of:

i. Extractive industries;
ii. Oil and gas services;
iii. Large scale infrastructure areas;
iv. Telecoms;
v. Pharmaceutical, medical device, and health care; and/or
vi. Financial services.

4. Transaction risk. Lawler says that this risk "first and foremost identifies and analyses the financial aspects of a payment or deal. This means that it is necessary to think about where your money is ending up." Red flags for transaction risk include:

i. High-reward projects;
ii. Involvement of many contractor or other third party intermediaries; and/or
iii. Projects without a clear legitimate object.

5. Business partnership risk. This prong recognizes that certain manners of doing business present more corruption risk than others. It may include:

   i. Use of third party representatives in transactions with foreign government officials;
   ii. A number of consortium partners or joint ventures partners; and/or
   iii. Relationships with politically exposed persons (PEPs).

There are a number of ways you can slice and dice your basic inquiry. As with almost all FCPA compliance, it is important that your protocol be well thought out. If you use one, some, or all of the above as your basic inquiries into your risk analysis, it should be acceptable as a starting point.

How should you assess your risks?

One of the questions that I hear most often is, "How does one actually perform a risk assessment?" Mike Volkov has suggested a couple of different approaches; he differentiates between smaller companies, which might use some basic tools such as "personal or telephone interviews of key employees; surveys and questionnaires of employees; and review of historical compliance information such as due diligence files for third parties and mergers and acquisitions, as well as internal audits of key offices", from larger companies. Such larger companies may use these basic techniques, but may also include a deeper dive into high-risk countries or high-risk business areas. If your company's sales model uses third-party representatives, you may also wish to visit with those parties or persons to help evaluate their risks for bribery and corruption that might well be attributed to your company.

Another noted compliance practitioner, William Athanas, took a different look at risk assessments. He posited that companies assume FCPA violations follow a "bell-curve distribution, where the majority of employees are responsible for the majority of violations".[3] However, Athanas believed that the distribution pattern more closely follows a "hockey-stick distribution, where a select few… commit virtually all violations". Athanas suggests assessing those individuals with the opportunity to interact with foreign officials who therefore also have the greatest chance to commit FCPA violations. Diving down from that group, certain individuals also possess the necessary inclination, whether a personal financial incentive linked to the transaction or the inability to recognize the significant risks attendant to bribery.

To assess these risks, Athanas suggested an initial determination of the touch-points where the operations of manufacturing companies "intersect with foreign officials vested with discretionary authority." This will lead to an understanding of the individuals who hold these roles within a company. This means that a simple geographic analysis is but a first step in a risk analysis. Thereafter, companies should also focus on "those who authorize and record disbursements, as well as those who represent the company in situations where they may be solicited for payments". The next step is to determine those company employees who may have the incentive "to pay bribes on the Company's behalf". This incentive can come in a variety of forms, such as a company compensation plan, which rewards high producers; employees who do not understand the risk they place the company (and themselves) in by engaging in activities which violate the FCPA; and, finally, those employees who seek to place their individual interests above those of the company.

Athanas concludes by noting that this limited group of employees, or what he terms the "shaft of the hockey-stick", is where a company should devote the majority of its compliance resources. With a proper risk assessment, a company can then focus its compliance efforts on "intensive training sessions or focused analysis of key financial transactions – on those individuals with the opportunity and potential inclination to violate the statute". This focus will provide companies with the greatest "financial value and practical worth of compliance efforts".

Lawler suggests that you combine the scores or analysis you obtain from the corruption markers you review, whether it is the DOJ list or those markers under the UK Bribery Act. From there, create a "rudimentary risk-scoring system that ranks the things to review using risk indicators of potential bribery". This ensures that high-risk exposures are done first and/or given more time. As with all populations of this type, there is likely to be a normal or "bell curve" distribution of risks around the mean. So 10-15 per cent of exposure falls into the relatively low-risk category; the vast majority (70-80 per cent) into the moderate-risk category; and the final 10-15 per cent would be high risk.

The desktop risk assessment

However, if you do not have the time, resources, or support to conduct a worldwide risk assessment annually, you can take a different approach. You might try assessing several areas annually through a more limited, focused risk

assessment, which a colleague of mine calls the "desktop risk assessment". Some of the areas that such an assessment could inquire into might be the following:

- Are resources adequate to sustain a culture of compliance?
- How are the risks in the C-suite and the boardroom being addressed?
- What are the FCPA risks related to the supply chain?
- How is risk being examined and due diligence performed at the vendor/agent level? How is such risk being managed?
- Is the documentation adequate to support the program for regulatory purposes?
- Is culture, attitude (tone from the top), and knowledge measured? If yes, can we use the information enhance the program?
- Disciplinary guidelines: Do they exist and has anyone been terminated or disciplined for a violating policy?
- Communication of information and findings: Are escalation protocols appropriate?
- What are the opportunities to improve compliance?

There are a variety of materials at your company that can facilitate such a desktop risk assessment. You can review your company's policies and written guidelines by reviewing anti-corruption compliance policies, guidelines, and procedures to ensure that compliance programs are tailored to address specific risks such as gifts, hospitality and entertainment, travel, political and charitable donations, and promotional activities.

You could assess your company's senior management support for your compliance efforts through interviews with high-level personnel such as the chief compliance officer (CCO), chief financial officer (CFO), general counsel (GC), head of sales, CEO, and board audit or compliance committee members to assess "tone from the top". You can examine resources dedicated to compliance and also seek to understand the compliance expectations that top management is communicating to its employee base. Finally, you can gauge operational responsibilities for compliance.

Such a review would lead to the next level of assessment, which can be generally labeled "communications". You can do this by assessing compliance policy communication to company personnel, but even more so by reviewing such materials as compliance training and certifications that employees might

have in their files. If you have not yet done so, you should also take a look at statements by senior management regarding compliance, such as actions relating to terminating employees.

A key element of any best practices compliance program is internal and anonymous reporting. This means that you need to review mechanisms on reporting suspected compliance violations and then actions taken on any internal reports, including follow-ups to the reporting employees. You should also assess whether those employees who are seeking guidance on compliance for their day-to-day business dealings are receiving adequate and timely responses.

I do not think there is any dispute that third parties represent the highest risk to most companies under the FCPA, so a review of your due diligence program is certainly something that should be part of any risk assessment. But more than simply a review of procedures for due diligence on third party intermediaries, you should also consider the compliance procedures in place for your company's mergers and acquisitions (M&A) team, focusing on the pre-acquisition phase.

One area that I do not think gets enough play, whether in the FCPA commentary or in day-to-day practice, is looking at what might be called "employee commitment" to your company's compliance regime. So here you may want to review your compliance policies regarding employee incentives for compliance. Just as you look at the carrots to achieve compliance with your program, you should also look at the stick, in the form of disciplinary procedures for violations. This means you should see if there have been any disciplinary actions for employee compliance violations, and then determine if such discipline has been applied uniformly. If you discipline top sales people in one company location, you have to discipline your top sales folks in all other locations for the same or similar violations.

This list is not intended to be a complete list of items, you can pick and choose to form some type of desktop risk assessment, but hopefully you can see some of the areas you can assess and deliver any remedial action that may be warranted. Further, if you aim to perform an annual desktop risk assessment, with a full worldwide risk assessment every two years or so, you should be in a good position to keep abreast of compliance issues that may change and need more or better risk management. Also, do not forget that the FCPA Guidance ends its section on risk with the following essential point: "When assessing a company's compliance program, DOJ and SEC take into

account whether and to what degree a company analyzes and addresses the particular risks it faces."

Engage and educate: A different model for a risk assessment

A completely different approach to risk assessment was articulated by Leonard Shen, vice president (VP) and chief compliance officer (CCO) at PayPal, in a presentation to Compliance Week 2012. His approach is not the right approach for every company, but for those initiating their compliance journey, or a company considering a significant compliance program enhancement, this approach may be more effective than the traditional risk assessment, where a team of lawyers, CPAs, and internal auditors assess a company's compliance environment.

In a company initiating its compliance program, it can be perceived as a sea change of culture. However, Shen indicated that he had used an approach which worked to alleviate those types of concerns, and which also provided enough information to perform a robust assessment that could be used to form the basis of an effective compliance program. He termed this type of approach as one to "engage and educate". While the approach had a two-word name, it actually had three purposes:

1. To engage the employees in what would form the basis for an enhanced compliance program;
2. To educate the employees generally in compliance and ethical behavior; and
3. Through the engagement of employees, to gather information which could be used to form the basis of a risk assessment.

Engagement

Shen and his compliance team traveled to multiple company locations across the globe to meet with as many employees as possible. A large number of these meetings were in town hall settings, and key employee leaders, key stakeholders, and employees identified as high risk due to interaction with foreign governmental official touch-points, were met with individually or in smaller groups. Shen and his team listened to their compliance concerns and more importantly took their compliance ideas back to the home office.

From this engagement, the team received several thousand employee suggestions regarding enhancements to the company's compliance program.

After returning to the US, Shen and his team winnowed down this large number to a more manageable number, somewhere in the range of 200. These formed the basis of a large core of the enhancements to the existing company compliance program. After the enhanced compliance program was rolled out, formal training began. During the training, the team was able to give specific examples of how employee input led to the changes in the enhanced program. This engaged the employees and made them feel like they were a part of, and had a vested interest in, the company's compliance program. This employee engagement led to employee buy-in.

Education

During the town hall meetings and the smaller more informal group meetings, Shen and his team were doing more than simply listening, they were also training. However, the training was not on specific compliance provisions; it was, more generally, on ethics and how the employees could use compliance as a business tool. Most ethical standards of a company are not found in an existing compliance program; they are found in the general anti-discrimination guidelines and ethical business practices such anti-competitiveness and prohibitions against the use of customer confidential information. Often, these general concepts can be found in a company's overall code of conduct or similar statement of business ethics; workplace anti-discrimination and anti-harassment guidelines can be found in human resource policies and procedures.

Shen and his team's aim for the education component of "engage and educate" was to encourage the company employees to start thinking about doing business the ethical way. It was ethical concept-based training designed to be in contrast with a rules-based approach where employees believe they are taught the rules, and then try to see how close they can get to the line of violating the compliance rule without actually stepping over the line. Moreover, this general ethical business training laid the groundwork for the enhancement of the company's compliance program, and the training that would occur when the enhancement was rolled out.

Risk assessment

A third key component of the "engage and educate" program is the risk assessment. Shen's approach here was not the traditional control testing model, where documents are pulled and tested against a standard. Instead, Shen

and his team listened, listened, and listened. They listened to their employees concerns and they listened to the compliance issues they raised. As they were listening, they began to ask questions about what was done and why. The questioning was not in an adversarial, interrogation mode, but rather ferreting out the employees' concerns while having the employees educate the team on the actual procedures that were used in several areas identified as key high risk.

Shen emphasized that this was an assessment and not an audit so no detailed forensic work was needed or used. However, by listening and gently questioning, Shen and his team were able to garner enough information to create a risk assessment profile that *informed* and became the basis of their compliance program enhancement. Shen and his team did not highlight to the company's employees that they were engaged in a formal risk assessment. He believed that, in many ways, he and his team were able to garner more useful information with which to inform their compliance program enhancement.

Shen's "engage and educate" approach worked for his company at that point in time. It may not work for other companies so well as a traditional risk assessment, but it does provide a different model if your company is beginning to create their compliance program, or is looking into a major enhancement. I recommend that you consider it.

How do you evaluate a risk assessment?

Mike Volkov has advised that you should prepare a risk matrix detailing the specific risks you have identified and relevant mitigating controls. From this, you can create a new control or prepare an enhanced control to remediate the gap between specific risk and control. Finally, through this risk matrix you should be able to assess relative remediation requirements. One way to do so was explored by Tammy Whitehouse in her assessment of the risk evaluation process used by Timken Company (Timken).[4]

Once risks are identified, they are rated according to their significance and likelihood of occurring, and then plotted on a heat map to determine their priority. The most significant risks with the greatest likelihood of occurring are deemed the priority risks, which become the focus of the audit/monitoring plan, she said. A variety of solutions and tools can be used to manage these risks going forward, but the key step is to evaluate and rate these risks.

Likelihood

Likelihood rating	Assessment	Evaluation criteria
1	Almost certain	Highly likely, this event is expected to occur
2	Likely	Strong possibility that an event will occur and there is sufficient historical incidence to support it
3	Possible	Event may occur at some point, typically there is a history to support it
4	Unlikely	Not expected but there is a slight possibility that it may occur
5	Rare	Highly unlikely, but may occur in unique circumstances

"Likelihood" factors to consider: the existence of controls, written policies and procedures designed to mitigate risk; capability of leadership to recognize and prevent a compliance breakdown, compliance failures, or near misses; training and awareness programs.

Priority

Priority rating	Assessment	Evaluation criteria
1-2	Severe	Immediate action is required to address the risk, in addition to inclusion in training and education and audit and monitoring plans
3-4	High	Should be proactively monitored and mitigated through inclusion in training and education and audit and monitoring plans
5-7	Significant	
8-14	Moderate	
15-19	Low	Risks at this level should be monitored but do not necessarily pose any serious threat to the organization at the present time.
20-25	Trivial	

Priority rating is the product of "likelihood" and significance ratings, reflecting the significance of a particular risk universe. It is not a measure of compliance effectiveness or a means to compare efforts, controls, or programs against peer groups.

At Timken, the most significant risks with the greatest likelihood of occurring are deemed to be the priority risks. These "severe" risks become the focus of the audit monitoring plan going forward. A variety of tools can be used, such as continuous controls monitoring with tools like those provided by Visual RiskIQ, relationship-analysis-based software such as Catelas, or other analytical based tools. But you should not forget the human factor. At Timken, one of the methods used by the compliance group to manage such risk is by providing employees with substantive training to guard against the most significant risks coming to pass, and to keep the key messages fresh and top of mind. The company also produces a risk control summary that succinctly documents the nature of the risk and the actions taken to mitigate it.

The key to the Timken approach is the action steps prescribed by their analysis. This is another way of saying that the risk assessment *informs* the compliance program, not vice versa. This is the method set forth by the DOJ in its FCPA Guidance and in the UK Bribery Act's "adequate procedures". I believe that the DOJ wants to see a reasoned approach with regards to the actions a company takes in the compliance arena. The model set forth by Timken certainly is a reasoned approach and can provide the articulation needed to explain which steps were taken.

Carol Saint, vice president of internal audit for 7-Eleven, who was interviewed by OCEG President Carol Switzer for an article in *Compliance Week*, described the company's approach: "We start with a risk assessment, beginning with business units because this is how the organization has designed accountability. We decompose business units into the processes and sub-processes they own and execute. We evaluate how sub-processes align to achievement of strategic objectives: How do they affect the company's value drivers? Next, we map financial statement lines to the sub-processes to help prioritize from that lens. Finally, for each sub-process we consider specific risks that could hinder achievement of strategic objectives, as well as fraud risks, significant accounting estimates, benchmarking/hot topics, and ERM risks. We created an "intensity rating" that measures how often a process/sub-process was mentioned in our stakeholder interviews as a risk to the company. And we also considered how cross-functional a process is so that the element of

complexity—a risk accelerator—could help determine audit plan priorities. This year's plan development process was quite intense, but I think we did a good job of creating a baseline so that future risk assessments are more efficient."[5]

References

1. United States & SEC v. Metcalf & Eddy, Inc., C.V. No. 99-12566-NG (D. Mass. Dec. 14, 1999).
2. Volkov, M., "Practical Suggestions for Conducting Risk Assessments", *Corruption, Crime & Compliance*, 1 May 2013, see corruptioncrimecompliance.com/2013/05/practical-suggestions-for-conducting-risk-assessments.
3. Athanas, W.C., "Rethinking FCPA Compliance Strategies in a New Era of Enforcement", *Industry Week*, 2 May 2011, see www.industryweek.com/articles/rethinking_fcpa_compliance_strategies_in_a_new_era_of_enforcement_24020.aspx.
4. Whitehouse, T., "Improving Risk Assessments and Audit Operations", *Compliance Week*, 7 June 2011, see www.complianceweek.com/news/news-bulletin/improving-risk-assessments-and-audit-operations.
5. The interview by Switzer is included in Medford, J., "Lessons on Risk Assessments from Winnie The Pooh", *Compliance Week*, 26 August 2014, see www.complianceweek.com/news/news-bulletin/lessons-from-winnie-the-pooh-on-risk-assessments.

Chapter 5: Getting out on the road – Training and continuous advice

Training

The communication of your anti-corruption compliance program is something that must be done on a regular basis to help ensure its effectiveness. The FCPA Guidance explains, "Compliance policies cannot work unless effectively communicated throughout a company. Accordingly, DOJ and SEC will evaluate whether a company has taken steps to ensure that relevant policies and procedures have been communicated throughout the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners."

"Conducting effective training programs" is listed in the 2011 US Sentencing Guidelines as one of the factors the DOJ will take into account when a company accused of a FCPA violation is being evaluated for a sentence reduction. The US Sentencing Guidelines mandate, "(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities."

OCEG President Carol Switzer, in an article entitled "Playing the Game of Risk in Workplace Education", laid out some excellent parameters for anti-corruption compliance training, beginning with the admonition that "one size does not fit all in deciding the content and intensity of training needs for each role or individual". Recognizing a risk-based analysis of who needs the training is just the start, Switzer believes that by engaging employees in the training, it can become more effective. She looks at "gamifying training", arguing, "Well-designed games encourage engagement, and more engagement means more

reinforcement, and that leads to better recollection and application of the information. Situational decision making drives the player to think, not just act. Making wrong choices and seeing the consequences leads to desire to act the right way and gain rewards, be it advancing to the next level of the game, earning a prize for success, or understanding that in the real workplace world the reward may be achievement of personal and organizational objectives." She articulated a three-pronged approach: define, design, and deliver.

Define

The first step is to define what you are trying to achieve. The approach recognizes that "while some organizations limit their training programs to what is legally required, more successful ones know that there are many reasons for developing a thoughtful, well-designed approach to employee education". Switzer posits that if a company's training is done right, it will help the organization to achieve several goals. These include: the business objectives; managing threats and business opportunities; addressing change in positive manner; helping to ensure integrity and the company's reputation; strengthening the business's culture and ethical conduct; and, lastly, providing evidence that the company has complied with legal requirements, such as the US Sentencing Guidelines and the ten hallmark's of an effective compliance program.

Design

The next step is to design the training program, which is further broken down into three steps, which drill down into the specifics of training. By using these three steps, you can help to ensure that the training will be effective for the individual, but also for the nature of the risk involved.

The first step is to design the training program. Steps include the development of curriculum using a risk-based model. You should set uniform methods for acquiring content, maintaining records, and reporting. This should be followed by the establishment of standards for selecting appropriate content, delivery methods, frequency, and assurance based on risk exposure. You can review any technological solutions for both e-learning delivery and documentation. Finally, you will need to consider training content revision when requirements or risk analyses change.

After the design of the training program, the next level is to design the specific training courses. Here you should establish your learning objectives and map the training to legal and competency requirements. You must always

remember who your audience is and what their characteristics might be. You need to ensure that the content is timely and the instructors are effective. Finally, you will need to not only determine the most appropriate mechanism to deliver the content, but also to define the key performance indicators and determine methods to audit them.

The final design level is the individual's training plan. Here you need to analyze what the person's role is within the organization and use this to determine mandatory and risk-based training needs. You will need to consider modifying the risk profile based upon assessments given before and after the training is delivered and then adapt the training as an employee's role and risk profile changes within an organization.

Deliver

For the delivery of the training materials, Switzer has laid out a tripartite scheme, breaking it down into high-risk exposure roles, medium-risk exposure roles, and low-risk exposure roles.

High-risk exposure roles

These are defined as those employees whose roles in an organization can significantly impact the company. Here expert subject proficiency is demanded and individuals should be able to act with confidence in a wide range of scenarios and conditions based on a strong understanding of the risks, requirements, and penalties. Training may be repeated frequently using several methods of delivery, have greater assurance through testing and certification of course completion, and include ongoing risk profiling of individuals through assessment of behavior choices in online courses or live simulation exercises.

Medium-risk exposure roles

These are defined as those employees who face risk on regular basis or present a moderate level of negative impact to a company if they mishandle the risk. These individuals should know the risks, requirements, and penalties, and should be able to apply their knowledge to common scenarios using standards and tools given to them. Training should have content to make these employees proficient in the subject, be refreshed periodically, use a variety of modes of delivery, and have methods to provide evidence of understanding.

Low-risk exposure roles

These are defined as those employees with a low likelihood of facing risk. Persons in this category should be made aware of any risks, requirements, and penalties, as well as the organization's expectations about how to address these. They should know relevant policies and procedures and where to get assistance in addressing a risk or making a behavior decision.

Evaluation of FCPA compliance training

One of the key goals of any FCPA compliance program is to train company employees in awareness and understanding of the FCPA and your specific company compliance program, and to create and foster a culture of compliance. The testing and evaluation of your FCPA compliance training program is an important aspect not to be overlooked. In their book entitled *Foreign Corrupt Practices Act Compliance Guidebook*, authors Martin and Daniel Biegelman explore some techniques which can be used evaluate FCPA compliance training.[1]

While most people tend to overlook the issue of attendance at training, it is an issue that should also be considered. You should determine that all senior management and company board members will have attended FCPA compliance training. You should review the documentation of attendance and confirm this attendance. Make your department, or group leaders, accountable for the attendance of their direct reports and so on down the chain. Evidence of training is important to create an audit trail for any internal or external assessment or audit of your training program.

The authors encourage post-training measurement of employees who participated. A general assessment of those trained on the FCPA and your company's compliance program is a starting point. They list five possible questions as a starting point for the assessment of the effectiveness of your FCPA compliance training:

1. What does the FCPA stand for?
2. What is a facilitation payment and does the company allow such payments?
3. How do you report compliance violations?
4. What types of improper compliance conduct would require reporting?
5. What is the name of your company's chief compliance officer?

The authors set out other metrics which can be used in the post-training evaluation phase. They point to any increase in hotline use as an indication of effective training: are there more calls into the compliance department requesting assistance or even asking questions about compliance? Is there any decrease in compliance violations or other acts of non-compliance?

End of training "flea dip"

Another approach comes from James Nortz, which he set out in an article entitled "Rethinking the Annual Compliance and Ethics Flea Dip".[2] Nortz characterized the annual compliance training program that most US companies' employees receive as a "flea dip". While he believes that such annual training is well-intentioned, he states that it is "a bit implausible that these annual pilgrimages" would have their intended effect of raising overall employee awareness of their company's code of conduct, and thereby reducing overall enterprise compliance risks.

Nortz cites two major reasons for this educational failure. The first is that "most compliance and ethics presentations anesthetize all but the most caffeinated, and are utterly unforgettable". To drive this point home, he challenges the reader to recall "even one PowerPoint slide" of the most recent compliance and ethics training presentation that they may have attended. The second reason is that, to truly affect behavior and get employees to understand the relevance of company codes of conduct, Nortz believes that a "different approach to teaching and learning is required". He believes that the recently developed "Learning IFF Action Model" could offer a better method for success in compliance and ethics training.

He defines "IFF" as "learning *in*, *from* and *for* action". In the IFF model, teaching is rooted in "both cognitive learning theory and common sense". Under this teaching theory, real-life experiences are incorporated into classroom training to reflect employees' experiences out in the business world. Nortz believes that such training is more beneficial in the compliance and ethics arena "where old habits are difficult to change and the application of even simple rules to circumstances that arise in the workplace can present complex, difficult challenges".

Nortz suggests moving away from a full and thorough discussion of relevant laws, whether they are your company's internal code of conduct or the FCPA. He suggests that compliance and ethics training should be integrated into more routine employee training rather than stand alone

compliance and ethics training. The more innovative component of Nortz's suggestions revolves around employee involvement and follow-ups. He believes that employees should be encouraged to share their experiences of how a company's code of conduct "come[s] into play and affect[s] the way they do their jobs" with other employees. The second component is to require employees, at periodic intervals, to meet with one another and their direct managers "to reflect and discuss how they handled particular situations in which the company code of conduct may have come into [play]". He re-emphasizes that such discussions can be best held in a routine business meeting and that it is not necessary to wait for any annual compliance and ethics training.

Nortz ends by noting that the IFF approach will require "considerably more thought and energy" than the traditional training approach, which usually involves using PowerPoint slides as the primary training materials. However, as Notes states, "if you are truly interested in ridding your company of 'fleas,' it may be a good idea to try an approach like the IFF learning model, which provides a more reasonable prospect of actually working".

Training to resist a bribe

Another approach is to provide some real-world practical examples of how employees can personally combat bribery and corruption. Using the white paper "Resisting Extortion and Solicitation in International Transactions" (RESIST) as a guidepost, you can train employees to respond appropriately to a variety of solicitations. Below are listed some responses to demands for these types of payments, as well as steps to address major aspects of these individual risks.

Demand response: How to react if such a demand is made?

Immediate response

- Take time to think about the situation, do not act alone, and stick to your mandate;
- Answer that the solicitation (direct or indirect) is to be made in writing and needs to be reported to your management; and
- Refuse payment on the grounds that any solicitation violates the business principles of your company.

Report internally

- Immediately report to management or the compliance department assigned with matters involving the code of conduct and define an appropriate strategy; and
- Record the incident and make an internal assessment to define corrective actions.

Investigate

- Investigate the deal and the intermediary, as well as past deals with the same counterparties and/or intermediary in same country or even other countries;
- Include legal, operational, and risk management specialists; and
- Retain investigation results for both legal implications and future risk assessments.

Discuss with the relevant parties

- Go back to the soliciting person or his/her superior with at least one witness with the following position: management; adviser; bank representative. Reaffirm your willingness to do business, perform the project or transaction, carry out the activity, and ignore the solicitation;
- Report (directly or anonymously) to the appropriate level of the organization allegedly represented by the person demanding the bribe;
- Explain to the persons making the solicitation that the proposed scheme could expose all the parties (individual and company) to a prosecution risk, not only in the country where the deal occurs but also in other countries under their laws prohibiting bribery and corruption or money laundering; and
- Convene meetings of all parties and discuss potential challenges to successful dealings such as requests for bribes, without disclosing too many details – this should serve as a deterrent to the guilty party.

If suspicions are substantiated, disclose externally

- Government: Use various governmental agencies to report corrupt organizations;

- Embassy or consulate representing your home country: Seek guidance and support;
- Financing institutions: If any export credit financing or coverage is proposed;
- Competitors: If they are subject to a regulatory environment similar to yours; and
- Industry trade association in the host country: Report on a "no name" basis and in a collective manner such solicitation to relevant authorities.

Withdraw

- Withdraw from the project or transaction and disclose the reasons for the withdrawal to the public, to international organizations, and/or selected officials of the country organizing the tender.

Communication

Ethical leadership is absolutely mandatory to have a successful compliance program, whether it is based upon the FCPA or the UK Bribery Act. Senior management must not only be committed to doing business in compliance with these laws, but they must communicate these commitments down to the organization. "Leadership" is not limited only to senior management within an organization. As discussed in Chapter 1, "tone at the top" begets "tone in the middle", which begets "tone at the bottom". At each rung, there is the need for compliance leadership. In an article in the *Harvard Business Review*, Boris Groysberg and Michael Slind discuss how to improve employee engagement in today's "flatter, more networked organizations".[3]

The authors posit that the issue of *how* leaders handle communications within their organizations is as important as the message itself. They believe that the process should be more dynamic and more nuanced, more "conversational". Building on this concept, they suggest a model of leadership, which they call "organizational conversation", and which in many respects resembles ordinary person-to-person conversations. They believe that this model has several advantages, including that it allows a large company to function like a small one, and that it can enable leaders to "retain or recapture some of the qualities… that enable start-ups to out-perform better established rivals". The authors have found four elements of organizational conversation which "reflect the essential attributes of an interpersonal conversation". They are: intimacy, interactivity, inclusion, and intentionality.

Intimacy: Getting close

Here, the authors appear to focus on two works: listening and authenticity. Recognizing that physical proximity may not always be feasible but emotional or mental proximity is required, they advise leaders to "step down from their corporate perches and then step up to the challenge of communicating personally and transparently with their people". This technique shifts the focus of change from a top-down hierarchical model to a "bottom-up exchange of ideas".

Interactivity: Promoting dialogue

Interactivity should make a conversation open and more fluid. You can obtain this by talking *with* and not just talking *to* an employee. The purpose of interactivity builds upon the first prong of intimacy. The authors believe that efforts to close the gap between employees will founder if tools are not in place, along with institutional support which gives employees the freedom and courage to speak up. The authors believe that social media can be a useful tool to help foster such interactivity, but care must be taken to ensure that managers do not simply use social media as another megaphone. The authors suggest that more than just social media is required and that something extra is needed, and that is social *thinking*.

Inclusion: Expanding employees roles

Following on from intimacy is inclusion, as intimacy should force a leader to get closer to employees while inclusion challenges the employee to play a greater role in the communication process. Inclusion expands on interactivity by enabling employees to put forward their ideas "rather than simply parrying the ideas that others present". Clearly, this is the prong that brings employee engagement into the communication process by calling on employees to "generate the content that makes up a company story". Employees who become committed to a message can become the best brand ambassadors that a company can ever hope to have on its payroll.

Intentionality: Pursuing an agenda

While the first three prongs of the authors' model focus on opening up the flow of communication, intentionality is designed to bring a measure of closure to the process. The goal here is to have voices merge into a single vision of what the company's communication stands *for*. In other words, the conversation

should reflect a "shared agenda that aligns with the company's strategic objectives" and will allow employees to "derive a strategically relevant action from the push and pull of discussion and debate". The leaders role here is to "generate consent rather than commanding assent" for a strategic objective. The authors believe that this enables employees at the top, in the middle, and at the bottom to "gain a big-picture view of where their company stands" on any issue which has gone through the process.

Company events

During its annual celebration of the week designated as "compliance and ethics week", one company I know uses this event as a springboard to internally publicize its compliance program. Their efforts included three separate yet inter-related initiatives: hosting inter-company events to highlight the company's compliance program; providing employees with a brochure highlighting the company's compliance philosophy and circulating a booklet which provides information on the company's compliance hotline and compliance department personnel.

These were "lunch 'n' learn" events hosted throughout the week. Topics included:

- Monday: Navigate and learn the corporate compliance website;
- Tuesday: How to determine if you have a conflict of interest;
- Wednesday: Review of the company's pre-approval procedures for gifts, travel, and entertainment of non-US officials and employees of state-owned enterprises;
- Thursday: Understanding the purpose and importance of the company's alert line; and
- Friday: Ethical behavior that wins business and attracts top talent.

Participation in these events allowed the compliance department to meet informally with the business unit folks. Even in a corporate headquarters, most conferences equate to more formalized training, but the "lunch 'n' learn" concept provides a more casual atmosphere and, therefore, better opportunities for interaction.

Cost: Sandwiches for lunch

Brochure

The company regularly distributes a short compliance brochure. In the brochure, which announced the company's celebration of compliance week, it included the following phraseology that I quote in its entirety as I thought it was so eye-catching. The brochure spelled out "compliance" vertically and assigned phrases to each letter so that it reads as follows:

Commit to "doing the right thing"
Observe the policies that apply to your job
Make compliance awareness a part of your job
Put code of conduct in accessible place
Lead by example
If in doubt, check it out
Attend educational and mandatory training sessions
Notify your supervisor of possible wrongdoings
Communicate openly and honestly
Ethics is a part of all activities

In addition to the above phrasing, the brochure included information on the company hotline, contact information for the compliance department and a listing of some of the information available on the company's internal intranet site.

Cost: Printer paper

Compliance booklet

The final piece of information provided during the company's compliance week celebration was a four-page booklet provided to each employee, specifically tailored to the celebration. It listed several elements from the company's compliance program and the company's "vision" and "core values". One of the most interesting things it listed was the compliance department philosophy about what it believed it owed the company's employees. This included the following:

- Guidance on the policies and procedures that apply to your duties;
- Training to enable your compliance with all applicable policies and procedures;
- Monitoring to ensure compliance with policies, procedures, and laws; and

- An environment that will not tolerate retaliation against those who report compliance concerns in good faith.

Cost: Thick printer paper

The key to training and communication is that they be done *effectively*. Whether you utilize one of the myriad of compliance training professionals, online training companies, or another mechanism, the bottom line is that you need to risk rank your training attendees and follow up by measuring training effectiveness. If you can neither think of anything else nor find the budget for professional consultants, you can always start with the FCPA Guidance and use the hypotheticals here as your training materials. I still maintain that, in communications, you are only limited by your own imagination. By keeping the communications fun, fresh, and relevant, you can help keep attention on compliance in your organization.

References

1. Biegelman, M., and Biegelman, D., *Foreign Corrupt Practices Act Compliance Guidebook*, Hoboken, N.J.: Wiley, May 2010.
2. Nortz, J., "Rethinking the Annual Compliance and Ethics Flea Dip"
3. Groysberg, B., and Slind, M., "Leadership is a Conversation", *Harvard Business Review*, June 2012, see hbr.org/2012/06/leadership-is-a-conversation/ar/1.

Chapter 6: Do as I do and as I say – Hiring, incentive, and disciplinary measures

HIRING PRACTICES under the FCPA are not often given much thought or widely discussed. They have come up for discussion more recently because of the issues surrounding the hiring of sons and daughters of foreign government officials (most publicized in relation to JPMorgan Chase & Co., but numerous other companies' similar hiring practices are under regulatory scrutiny). As far back as 2004, in Opinion Procedure Release 04-02, the DOJ realized this was an important part of an overall compliance program when it approved a proposed program that had the following requirement: "Clearly articulated procedures which ensure that discretionary authority is not delegated to persons who the company knows have a propensity to engage in illegal or improper activities."[1]

I thought about some of these issues when I read a recent "The Saturday Essay" in the *Wall Street Journal*, entitled "How to Trick the Guilty and Gullible into Revealing Themselves". In this essay, which they adapted from their most recent book *Think Like a Freak*, Steven Levitt and Stephen Dubner, compare two diverse tactics used by King Solomon and the band Van Halen to see who might be telling the truth, or not, in a specific situation. In the oft-told tale, King Solomon decreed that he would split a baby in two and give one-half each to two women who claimed to be the mother; the true mother told him to give the baby to the other woman. King Solomon used this fact to determine who the real mother was. In the case of rock band Van Halen, they had a 53-page rider giving "point-by-point instructions" in in their touring contract. This rider had technical and security specifications for each venue the band played. It also had language in ALL CAPS that stated "M&M's (WARNING: ABSOLUTELY NO BROWN ONES)". Initially this language was derided as simply rock and roll excess to the hilt, but band member David Lee Roth explained that if he

went into the dressing room and found no brown M&Ms, it signified to him that the local promoter was telling the truth when he claimed to have read the contract. If there were brown M&Ms, the band had to perform extra reviews of the stage electrical and lighting setups.

Why is hiring so important under the FCPA? It is because hiring is important to any company's health and reputation. Like most areas of FCPA compliance, good hiring practices for those employees who will do business in compliance with anti-corruption laws such as the FCPA are simply good business practice. Levitt and Dubner cite the following statistic, "By one industry estimate, it costs an average of roughly $4,000 to replace a single employee, and one survey of 2,500 companies found that a single bad hire can cost more than $25,000 in lost productivity, lower morale and the like." In one company I worked for this estimate went as high as $400,000 to hire and fully train a new employee. I would add that those costs could go up significantly if a bad hire violates the FCPA.

Brooke Denihan Barrett, CEO of the Denihan Hospitality Group, interviewed in the *New York Times*, said that by the "time somebody meets me, you can assume that the skills are there. So what I interview for is fit. And I'm always very curious to know, what is it about our company that appeals to that person?"[2] She asks specifically about culture, requesting the candidate define it and how they think that culture is special. She also asks candidates to talk about a failure, how they dealt with the experience, what lessons that they learned from the it. I would suggest that both of those lines of inquiry should be used when evaluating a candidate for hire.

In a completely different arena, Houston Dash general manager Brian Ching talked about the expectations he and his club has for the female soccer players on the squad. In addition to the obvious requirement for a professional soccer player to be technically proficient in the game, the team expects each player to have significant community involvement to help develop a fan base for the club. In the player interview process, this is thoroughly explained and each prospective player is asked if they would be willing to take on this additional role. More than simply using this Q&A as an evaluation technique, it allows the team to communicate its expectations to each potential team member.

This is something that HR and others involved in the hiring process can take to heart. They should have a serious and frank discussion with all potential hires, particularly those going into senior management or FCPA-related high-risk

areas. This not only allows an evaluation along the lines that Barrett uses to determine if a hire will be a cultural fit for her company, but it permits a company to directly express its expectations surrounding FCPA compliance and doing business ethically if a person is hired.

Compliance due diligence checks: The reference interview

A compliance evaluation is becoming a more common component of the employee selection and hiring process. Many companies now specifically include background checks (or due diligence in compliance parlance) when hiring senior managers or others who will hold high levels of authority for a company. Many practitioners feel that a reference is not of value because prospective candidates will only list references they believe will provide glowing recommendations of character. This leads to a pro forma reference check. However, in a *Harvard Business Review* article, Kevin Ryan explodes this misconception by detailing how he views the entire hiring process and specifically checking references.[3]

In the hiring of personnel, Ryan details the three steps his company takes:

1. Resumé review;
2. In-person interview; and
3. Reference checks.

Ryan believes that resumes are good for establishing "basic qualifications for the job, but not for much else". He believes that the primary problem with in-person interviews is that they are skewed in favor of "persons who are well spoken [or] present well". For Ryan, the key check for essential qualities like attention to detail, teamwork, and collaboration is through references and he says that "References are really the only way to learn these things."[4]

Ryan recognizes that many people believe that reference checks are not of great value because companies cannot or will not give out much more information than confirming dates of employment. However, he also believes that "the way around it is to dig up people who will speak candidly". He also recognizes that if you only speak to the references listed on a resume or other application, you may not receive the most robust appraisal. Ryan responds that the answer is to put in the work to check out references properly. Ryan believes this is one of the key strengths of search firms and that companies should emulate this practice when it comes to reference checks.

He notes that anyone who has worked in an industry for any significant length of time will have made many connections. Invariably, some of these connections will be acquainted with you or those in your current, and former, company. Ryan gave the following example: a longtime friend who was employed at another company called and said that he had been asked by his hiring partner to find out "the real story" on a hiring candidate by asking Ryan his candid opinion of the candidate. Ryan's response was "don't hire him". Lest you think that such refreshing honesty no longer exists when informal employment references are provided, you are mistaken. In my past corporate position, I was charged in performing compliance due diligence on senior executives and I spent time doing what Ryan suggested: calling acquaintances that I knew and asking such direct questions. More than 75 per cent of the time, I got direct responses.

Ryan believes that you must invest in the hiring process to get the right people for your company. The same is true for compliance. You do not want people with a propensity for engaging in corrupt acts working for, or leading, your company. So give the reference check some respect, for if you respect it, it can be a valuable and useful tool for you and your compliance program.

Using HR to change your company's compliance DNA

Matt Kelly, Editor of *Compliance Week*, wrote about the interaction of compliance departments and human resources (HR).[5] He noted that while compliance departments may look to HR to support internal investigations, HR can also be used to assist in "molding company culture". However, it is rarely used for this function. I heartily agree with Matt's sentiments. In addition to supporting internal investigations, I believe that HR can be used in some of the following ways to assist the compliance department. It can be a key component in changing or maintaining your company's compliance DNA.

Training

A key role for HR in any company is training. This has traditionally been in areas such as discrimination, harassment, and safety, to name just a few, and, based on this traditional role, this commentator would submit that FCPA compliance and ethics training is a natural extension of HR's function.

Employee evaluation and compensation

What policy does a company take to punish those employees who may engage in unethical and non-compliant behavior in order to meet company revenue targets? Conversely, what rewards are handed out to those employees who integrate ethical and compliant behavior into their individual work practices going forward? One of the very important functions of HR is assisting management in setting the criteria for employee bonuses and in the evaluation of employees for those bonuses. This is an equally important role in conveying the company message of adherence to a FCPA compliance and ethics policy.

This requirement is codified in the US Sentencing Guidelines with the following language: "The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct."

Does a company have, as a component of its bonus compensation plan, a part dedicated to FCPA compliance and ethics? If so, how is this component measured and then administered? There is very little in the corporate world that an employee notices more than what goes into the calculation of their bonuses. HR can, and should, facilitate this process by setting expectations early in the year, and then following through when bonuses are released. With the assistance of HR, such a bonus can send a powerful message to employees regarding the seriousness with which compliance is taken at the company. There is nothing like putting your money where your mouth is for people to sit up and take notice.

One function of HR is to help ensure consistent application of company values throughout the organization, and this should not exclude those employees identified as "rising stars". Another important role for HR is to help build trust throughout the company and recognize the benefits which result from that trust. If a company has an employee who meets, or exceeds, all of his sales targets, but does so in a manner inconsistent with the company's stated FCPA compliance and ethics values, other employees will watch and see how that employee is treated. Is that employee rewarded with a large bonus? Is that employee promoted or are the employee's violations of the company's compliance and ethics policies swept under the carpet? If the employee is rewarded, both monetarily and through promotions, or in any way not

sanctioned for unethical or non-compliant behavior, it will be noticed and other employees will act accordingly.

Background screening

A key role for HR in any company is the background screening of not only employees at the time of hire, but also of employees who may be promoted to senior leadership positions. HR is usually on the front lines of such activities, although it may work in conjunction with the legal or compliance departments. These types of internal background checks can include a detailed review of employee performance; disciplinary actions, if any; internal and external achievements while employed by the company; and confirmation that the employee has both completed ethics and compliance training and the required annual compliance certification. A key internal function where HR can be an important lead is to emphasize that an employee who has been investigated but cleared of any alleged ethics and compliance violations should not be penalized.

When the government comes knocking

Another role for HR can be in the establishment and management of (1) an "amnesty program" or (2) a "leniency program" for both current and former employees. Such programs were implemented by Siemens during its internal bribery and corruption investigation. The amnesty program allowed appropriate current or former employees who fully cooperated and provided truthful information to be relieved from the prospect of civil damage claims or termination. The leniency program allowed Siemens employees who had provided untruthful information in the investigation to correct this information subject to individual disciplinary determinations. Whichever of these programs, or any variations, are implemented, HR can perform a valuable support role to legal and/or compliance.

Doing more with less

While many practitioners do not immediately consider HR as a key component of a FCPA compliance solution, it can be one of the lynchpins in a program to spread a company's commitment to compliance throughout the employee base. HR can also be used to "connect the dots" in many divergent elements in a company's FCPA compliance and ethics program. By asking HR to expand their traditional function to include the FCPA compliance and ethics function,

it can drive home the message of compliance at all levels within a company, from senior to middle management, and to those on the shop floor. HR focuses on behaviors, and by asking this department to emphasize compliant and ethical behavior, this will become part of a company's DNA.

Succession planning from the compliance perspective

Succession planning is not only a key issue for HR, it is also a key component of your compliance program. A.G. Lafley, writing in the *Harvard Business Review*, discussed the issue of succession planning during his tenure as the CEO of Procter & Gamble (P&G).[6] Many of the concepts and issues that Lafley discusses within the context of succession planning in general are applicable to compliance within this area.

Lafley's article makes clear that succession planning requires the same "coherence, discipline and thoroughness as governance, enterprise risk and strategic oversight". Sadly, many companies fail to give it the attention it requires. Indeed, in a PricewaterhouseCoopers survey, cited in the Executive summary to this report, nearly one half of the more than 1,000 directors gauged reported dissatisfaction with their companies' succession plans. Imagine what that number would be if they took into account the compliance aspect of succession planning.

Borrowing from Lafley, I have created Table 1, overleaf, for an analysis of some of the characteristics that should be considered in succession planning from the compliance perspective.

Lafley makes clear that succession planning does not begin at the time a CEO decides to retire. It should being at the time that a CEO is *hired*. This is to prevent a decision at the last minute or, worse yet, "to be left with effectively no decision". As well as the process being started at the time a new CEO is hired, it must also fully engage the board of directors. Lafley provides several key points, all of which are applicable to the compliance component of succession.

Lafley defines the evaluation process as an ongoing, not episodic, process. In addition to a "broad and deep pipeline of qualified leaders" the candidates should be put through a variety of roles. In the compliance context, this would provide an opportunity to review the initiatives and responses in several different areas. In addition to running large and small business units, such candidates should oversee several different functions, from the chief financial officer (CFO) to HR.

	Personal judgement	Team judgment	Organizational judgment	Stakeholder judgment
People	Personal judgments about overall compliance goals	Judgments regarding your team members regarding compliance	Judgments on organizational systems for assessing compliance with the organization	Judgments about how to engage stakeholders regarding compliance
Strategy	Personal judgments regarding compliance in your career	Judgments about how your team evolves in its compliance approaches as new compliance challenges arise	Judgments about how to engage and align all organization levels in compliance	Judgments in leading stakeholders to execute compliance strategies
Crisis	Personal judgments regarding compliance in times of crisis	Judgments on how your team operates regarding compliance in times of crisis	Judgments about how to work with your overall organization in terms of compliance in times of crisis	Judgments about dealing with key stakeholders regarding compliance in times of crisis

Table 1: Succession planning from a compliance perspective

In many ways, evaluating a compliance criterion is as much an art as it is a science. However, Lafley states that a specific list of "must-haves" is appropriate. It is not as simple as whether there has been a violation or not. It is broader than that. I often write about Paul McNulty's three "maxims" which are:

- Maxim No. 1: "What did you do to stay out of trouble?"
- Maxim No. 2: "What did you do when you found out?" and
- Maxim No. 3: "What remedial action did you take?"

Compliance for the CEO candidate is more than the third of these maxims. Evaluation should include: how did you integrate compliance into the business unit that you are managing? What controls did you put in place? And *then* what did you do when you found out about it?

Lafley defines this as "how the future might look". You might explore a new geographic market with a candidate or a new product line, either of which might bring new compliance challenges. Being a part of a team to perform a risk assessment might indicate that new or different compliance safeguards need to be considered. Should monitoring, through continuous controls monitoring or other more sophisticated tools, be utilized as the compliance program evolves?

Lafley points out that the choice of "a successor isn't a done deal until the votes are cast and the announcement is made". He advocates continuing to provide challenging projects, which would include those in the compliance arena, and which can continue to provide feedback and guidance from the compliance perspective. As one division president told me, "You are always being evaluated." This is as it should be. The selection of a new CEO is a substantial investment by a large company. Having the right person in the position from the compliance perspective is an important element in an overall evaluation. Remember: it all starts with the "tone from the top".

The fair process doctrine as a key component of a compliance program

Procedural fairness is one of the things that will bring credibility to your compliance program. Today it is called the "fair process doctrine" and this doctrine generally recognizes that there are fair procedures, not arbitrary ones, in processes involving rights. Considerable research has shown that people are more willing to accept negative, unfavorable, and non-preferred outcomes when they are arrived at by processes and procedures that are perceived as fair. Adhering to the fair process doctrine in two areas of your compliance program is critical for you as a compliance specialist, or for your compliance department, in order to have credibility with the rest of the workforce.

1. Internal investigations

The first area is that of internal company investigations. If your employees do not believe that the investigation is fair and impartial, then it is not fair and impartial. Further, those involved must have confidence that any internal

investigation is treated seriously and objectively. One of the key reasons that employees will go outside of a company's internal hotline process is because they do not believe that the process will be fair. This has been made even more important by the whistleblower provisions of the Dodd-Frank Act.

This "fairness" has several components. One would be the use of outside counsel, rather than in-house counsel to handle the investigation. Moreover, if company uses a regular firm, it may be that other outside counsel should be brought in, particularly if regular outside counsel has created or implemented key components which are now being investigated. Further, if the company's regular outside counsel has a large amount of business with the company, then that law firm may have a very vested interest in maintaining the status quo. Lastly, the investigation may require a level of specialization that in-house or regular outside counsel does not possess.

2. Administration of discipline and employee promotions

However, as important as the fair process doctrine is with internal investigations, I believe it is more important in another area. That area is in the administration of discipline after any compliance-related incident. Discipline must not only be administered fairly, it must be administered uniformly across the company for the violation of any compliance policy. It cannot matter that one employee is a friend of yours, or worse yet a "high producer". Failure to administer discipline uniformly will destroy any vestige of credibility that you may have developed.

In addition to the area of discipline which may be administered after the completion of any compliance investigation, you must also include compliance as a part of ongoing employee evaluations and the promotions process. If your company is seen to only advance and reward employees who achieve their numbers, by whatever means necessary, other employees will certainly take note and it will be understood that this is what management evaluates, and what employees are rewarded upon. I have often heard the (anecdotal) tale about some Far East regional manager, which goes along the following lines: "If I violated the code of conduct, I may or may not get caught. If I get caught I may or may not be disciplined. If I miss my numbers for two quarters, I *will* be fired". If this is what other employees believe about how they are evaluated and the basis for promotion, you have lost the compliance battle.

Implementing compliance incentives

Borrowing from an article in the Spring 2014 issue of the *MIT Sloan Management Review*, I have developed six core principles for incentives, adapted for the compliance function in an anti-corruption compliance program.[7]

1. Compliance incentives don't have to be elaborate or novel: The first point is that there are only a limited number of compliance incentives that a company can meaningfully target. Evidence suggests the successful companies are the ones that were able to translate pedestrian-sounding compliance incentive goals into consistent and committed action.
2. Compliance incentives need supporting systems if they are to stick: People take cues from those around them, but people can be fickle and easily confused; gain and hedonic goals can quickly drive out compliance incentives. This means that you will need to construct a compliance function that provides a support system to help them operationalize their pro-incentives at different levels, and thereby make them stick. The specific systems which support incentives can be tailored to your company, but the key point is that they are delivered consistently because this signals that management is sincere.
3. Support systems are needed to reinforce compliance incentives: One important form of a supporting system for compliance incentives is "to incorporate tangible manifestations of the company's pro-social goals into the day-to-day work of employees". Make the rewards visible. As stated in the FCPA Guidance, "Beyond financial incentives, some companies have highlighted compliance within their organizations by recognizing compliance professionals and internal audit staff. Others have made working in the company's compliance organization a way to advance an employee's career."
4. Compliance incentives need a "counterweight" to endure: Goal-framing theory shows how easy it is for compliance incentives to be driven out by gain or hedonic goals, so even with supporting systems it is quite common to see executives bowing to short-term financial pressures. Thus, a key factor in creating enduring compliance incentives is a "counterweight"; that is, any institutional mechanism that exists to enforce a continued focus on a nonfinancial goal. This means that in any financial downturn compliance incentives are not the first thing that gets thrown out the window, and if my hypothetical foreign regional manager misses his number for two quarters,

he does not get fired. So the key is that the counterweight has real influence; it must hold the leader to account.

5. Compliance incentive alignment works in an oblique, not linear, way: The authors state that "In most companies, there is an implicit belief that all activities should be aligned in a linear and logical way, from a clear end point back to the starting point. The language used — from cascading goals to key performance indicators — is designed to reinforce this notion of alignment. But goal-framing theory suggests that the most successful companies are balancing multiple objectives (pro-social goals, gain goals, hedonic goals) that are not entirely compatible with one another, which makes a simple linear approach very hard to sustain." What does this mean in practical terms for your compliance program? If you want your employees to align around compliance incentives, your company will have to "eschew narrow, linear thinking, and instead provide more scope for them to choose their own oblique pathway". This means emphasizing compliance as part of your company's DNA on a consistent basis, "the intention being that by encouraging individuals to do 'good,' their collective effort leads, seemingly as a side-effect, to better financial results. The logic of '[compliance first], profitability second' needs to find its way deeply into the collective psyche of the company."
6. Compliance incentive initiatives can be implemented at all levels: Who at your company is responsible for pursuing compliance incentives? If you head up a division or business unit, it is clearly your job to define what your pro-social goals are and to put in place the supporting structures and systems described here. But what if you are lower in the corporate hierarchy? It is tempting to think this is "someone else's problem", but actually there is no reason why you cannot follow your own version of the same process.

Looking for some specific compliance obligations to measure against? You could start with the following examples of compliance obligations that are measured and evaluated.

For senior management

- Lead by example, from your own conduct and in the decisions you take to the resources and time you commit to compliance;

- Facilitate and proactively practice in day-to-day activities the key compliance competencies, both internally and externally; and
- Support specific initiatives from the CEO, legal, and compliance functions.

For middle management

- Demonstrate, facilitate, and proactively practice in day-to-day activities the key compliance competencies, both internally and externally;
- Support specific initiatives from the legal and compliance functions;
- Ensure that all employees, agents, and contractors directly or indirectly reporting to you fully complete all required training and communications in a timely manner;
- Provide full cooperation with investigations conducted by the compliance or legal functions into any alleged violation of compliance policies;
- Include the chief compliance officer or another legal or compliance function representative in your management meetings at least twice per year, per geography;
- Identify instances of non-compliance and support compliance monitoring and reporting systems; and
- Partner with compliance in resolving compliance issues.

For business development or company sales representatives

- Certify that all employees, agents, and contractors directly or indirectly reporting to you have fully reported all sales and marketing interactions with all government officials in a timely manner;
- Certify that all employees, agents, and contractors directly or indirectly reporting to you have fully, promptly, and accurately reported all expenses with third party sales representatives that have occurred.

I started this chapter by talking about the role of HR in your anti-corruption compliance program. If it is not clear from reading this chapter, you need to put this book down and walk down the hall to the head of your company's HR function. They can be one of your best allies in your anti-corruption compliance program.

References

1. FCPA Opinion Procedure Release No. 04-02, 12 July 2004, see www.justice.gov/criminal/fraud/fcpa/opinion/2004/0402.pdf.
2. Bryant, A., "We're Family, Yes, but We're Still Accountable", *New York Times*, 11 May 2013, see www.nytimes.com/2013/05/12/business/brooke-denihan-barrett-on-family-and-business.html?_r=0.
3. Ryan, K., "Gilt Groupe's CEO on Building a Team of A Players", *Harvard Business Review*, January-February 2012, see hbr.org/2012/01/gilt-groupes-ceo-on-building-a-team-of-a-players/ar/1.
4. Ryan, K., "Gilt Groupe's CEO on Building a Team of A Players", in *Harvard Business Review*, How I Did It: Lessons from the Front Lines of Business, Harvard Business Review Press, March 2014.
5. Kelly, M., "The Hardest Department to Work With?", *Compliance Week*, 5 July 2011, see www.complianceweek.com/blogs/the-big-picture/the-hardest-department-to-work-with#.VBAImcJdU1I.
6. Lafley, A.G. "The Art and Science of Finding the Right CEO", *Harvard Business Review*, October 2011, see hbr.org/2011/10/the-art-and-science-of-finding-the-right-ceo/ar/1.
7. Birkinshaw, J., Foss, N.J., and Lindenberg, S., "Combining Purpose with Profits", *MIT Sloan Management Review*, Spring 2014, see sloanreview.mit.edu/article/combining-purpose-with-profits.

Chapter 7: Your greatest source of FCPA risk

IMAGINE YOU are sitting in your office and the CCO or GC comes in and says that the board of directors wants to have all of the company's third parties fully compliant with the company's anti-corruption compliance program within the next year (it is early in the year). He further says he would like your plan to go forward with this initiative by the end of the week (it is early in the week). After a quick call to your company's procurement function and finance function you find that there are multiple thousands of third parties, which are vendors in the supply chain or representatives in the sales chain. What can you do and where can you turn? I would propose that you think through how you might tackle such an assignment in what I call, "the lifecycle of third-party management".

Lest you think such a task is well-nigh impossible, consider the situation that confronted Tyco International. In an article in the September 2011 issue of *Compliance Week*,[1] author Karen Kroll reported Tyco's successful, "comprehensive program to gain a better control over the activities of third parties". The development of such a program was a tall order, as Tyco initially identified over 66,000 third-party vendors and this group needed to be risk assessed to determine the high-risk third parties which could be handled in the first pass. So there is at least one good example out there that you can draw on for inspiration.

Why is it even necessary for your company to develop a program to manage third parties? In a white paper, entitled "Third Party Essentials: A Reputation/Liability Checkup When Using Third Parties Globally", authors Marjorie Doyle and Diana Lutz suggest that in most foreign business partner relationships, your company will be held responsible for the actions of third parties working for and with your company. The new global expectation is that

"you know who they are, you have vetted them and you are in control of the activities for which you hired them". The authors further believe that this is even more important when anti-corruption and anti-bribery laws – such as the FCPA, UK Bribery Act, or other OECD-based legislation – are applicable. They note, "Gone are the days when organizations could wash their hands of liability or damage to reputation from outsourced work due to ethics and compliance failure."

It is generally recognized that third parties present the greatest risk under the FCPA. But for the DOJ, SEC, UK SFO, or other anti-corruption or anti-bribery regulator, the ultimate question is simply, does the system work? Questions about effectiveness, therefore, get to that core issue of whether all the compliance activities actually make the business less vulnerable to corruption risk. One thing that the DOJ and SEC have made clear in both FCPA enforcement actions and their jointly released FCPA Guidance is that a well-reasoned, thought out, and documented compliance regime will receive considerable weight in any review. The FCPA Professor, in his book *The Foreign Corrupt Practices Act in a New Era*, says that "a company should institute appropriate due diligence and compliance requirements pertaining to the oversight and retention of third parties". Based upon the need to systematically analyze and think through the management of third parties, I breakdown the lifecycle of third-party management into five steps:

1. Business justification and business sponsor;
2. Questionnaire to third party;
3. Due diligence on third party;
4. Compliance terms and conditions, including payment terms; and
5. Management and oversight of third parties after contract signing.

In this chapter, I will review each of these steps and provide specific guidance on how you should develop, implement, and execute them.

Step 1: Business justification

It really seems to me that it should be common sense for companies to have a business justification to hire or use a third party. If that third party is in the sales chain of your international business, it is important to understand why you need to have that particular third party represent your company. This concept is enshrined in the FCPA Guidance, which says "companies should

have an understanding of the business rationale for including the third party in the transaction. Among other things, the company should understand the role of and need for the third party and ensure that the contract terms specifically describe the services to be performed."

The Internal Revenue Service (IRS) also considers a business justification to be an important part of any best practices anti-corruption compliance regime. Clarissa Balmaseda, a special agent in charge of IRS criminal investigation, speaking at the 2013 ACI Bootcamp in Houston, said that lack of business justification should be a "red flag" for corruption. With the DOJ, SEC, and IRS all noting the importance of a business justification, it is clear that this is something you should incorporate into your compliance program.

However, the business justification also provides your company with the opportunity to help drive compliance into the fabric of your everyday operations. This is done by requiring the employee who prepares the business justification to be the business sponsor of that third party. The business sponsor can provide the most direct means of communication to the third party and can be the point of contact for compliance issues.

Tyco International takes this approach in its "seven-step process for third-party qualification". Tyco breaks the first step into two parts, which include:

1. Business sponsor: Initially identify a business sponsor or primary contact for the third party within your company. This requires not only business unit buy-in, but also business unit accountability for the business relationship – or as Scott Moritz, a partner at Navigant and one of the architects of the Tyco process, has said, "This puts the onus on each stakeholder."
2. Business justification: The business unit must articulate a commercial reason to initiate or continue to work with the third party. You need to determine how this third party will fit into your company's value chain and whether they will become a strategic partner or will be involved only in a one-off transaction?

Dan Chapman, the CCO at Parker Drilling, gave his thoughts on his company's 12-point evaluation process for reviewing, assessing, then contracting with and managing, foreign business partners. Under "step two", which he entitled, "competence of foreign business partner", he detailed a two-part analysis for his company, which "includes a review of the qualifications of the candidate for subject matter expertise and the resources to perform the services for which

they are being considered. However, it also in includes an identification of the representative's expected activities for your company."

He also added, under the step which he designated "business justification for use of agent and reasonableness of compensation", that "you should begin the entire process by requiring the relevant business unit which desires to obtain the services of any foreign business partner to provide you with a business justification including current opportunities in territory, how the candidate was identified and why no currently existing foreign business relationships can provide the requested services. Your next inquiry should focus on the terms of the engagement, including the commission rate, the term of the agreement, what territory may be covered by the agreement and if such relationship will be exclusive."

So, what should go into your business justification? First and foremost, you should craft a document that works for both you as the compliance practitioner and the business folks in your company. There are some basic concepts that I think are important, but you may want to modify my suggestions based on your own experiences.

You need the name and contact information for both the business sponsor and the proposed third party. You need to inquire into how the business sponsor came to know about the third party because it is a red flag if a customer or government representative points you toward a specific third party. You should inquire into what services the third party will perform for your company, the length of time, and the compensation rate for the third party. You will also need an explanation of why this particular third party should be used as opposed to an existing or other third party, if such were considered. All of this information should be written down and then signed by the business sponsor.

Remember, the purpose of the business justification is to document the satisfactoriness of the business case to retain a third party. The business justification should be included in the compliance review file assembled on every third party at the time of initial certification and again if the third party relationship is renewed.

Step 2: Questionnaire

Next is step 2, which I label as "the questionnaire". The term "questionnaire" is mentioned several times in the FCPA Guidance. It is generally recognized as one of the tools that a company should employ in its investigation to better

understand those with whom it is doing business. I believe that this requirement is not only a key step for you as a company, but also a mandatory step for any third party that desires to do work with your company. I tell clients that if a third party does not want to fill out the questionnaire, or will not fill it out completely, that you should not walk but run away from doing business with such a party.

In the 2011 UK Ministry of Justice's (MOJ), discussion of six principles of an "adequate procedures compliance program", the MOJ said the following about the questionnaire: "This means that both the business person who desires the relationship and the foreign business representative commit certain designated information in writing prior to beginning the due diligence process." Indeed, the use of a questionnaire was one of the key findings of Kroll's "2012 FCPA Benchmark Report". As reported in the FCPA blog: 71 per cent of companies surveyed require third parties to complete a disclosure, listing affiliations with foreign officials (65 per cent verify that third parties adhere to the company's code of ethics and 73 per cent confirm that each third party is free from sanctions pertaining to compliance with anti-bribery regulation).[2]

One of the key requirements of any successful anti-corruption compliance program is that a company must make an initial assessment of a proposed third-party relationship. The size of a company does not matter as small businesses can face quite significant risks and will need more extensive procedures than other businesses facing limited risks. The level of risk that companies face will also vary with the type and nature of the third parties with whom it may have business relationships. For example, a company that properly assesses that there is no risk of bribery on the part of one of its associated persons will, accordingly, require nothing in the way of procedures to prevent bribery in the context of that relationship. By the same token, the bribery risks associated with reliance on a third party agent representing a company in negotiations with foreign public officials may be assessed as significant and, accordingly, as requiring much more in the way of procedures to mitigate those risks. Businesses are likely to need to select procedures to cover a broad range of risks, but any consideration by a court of the adequacy of procedures in an individual case is likely to focus on those procedures designed to prevent bribery on the part of the associated person committing the offence in question.

So what should you ask for in your questionnaire? Randy Colrey, executive vice president (EVP) and global compliance officer at Edelmen Inc., said in a

presentation at Compliance Week 2012,[3] that his company has developed a five-step approach to evaluating and managing their third parties. In step 3, they ask, "What do you need to know?"

Initially, Corley said that scope of review depends on risk assessment: high risk, medium risk, or low risk. This risk ranking will determine the level of information collected and due diligence performed. The key element of this step is data collection. The initial step is to have the third party complete an application, which should include requests for information on background and relevant experience, scope of services to be provided, list of actual and beneficial owners, references, and compliance expertise.

Below are some of the areas into which I think you should inquire when evaluating a proposed third party:

- Ownership structure: Describe whether the proposed third party is a government or state-owned entity and the nature of its relationship(s) with local, regional, and governmental bodies. Are any members of the business partner related by blood to governmental officials?
- Financial qualifications: Describe the financial stability of, and all capital to be provided by, the proposed third party. You should obtain financial records, audited for three to five years, if available. Obtain the name and contact information for their banking relationship.
- Personnel: Determine whether the proposed agent will be providing personnel, particularly whether any of the employees are government officials. Make sure that you obtain the names and titles of those who will provide services to your company.
- Physical facilities: Describe what physical facilities will be used by the third party for your work. Be sure to obtain their physical address.
- References: Obtain names and contact information for at least three business references that can provide information on the business ethics and commercial reliability of the proposed third party.
- PEPs: Are any of the owners, beneficial owners, officers, or directors politically exposed persons (PEPs).
- UBOs: It is imperative that you obtain the identity of the ultimate beneficial owner (UBO).
- Compliance regime: Does the proposed third party have an anti-corruption/anti-bribery program in place? Do they have a code of conduct? Obtain copies of all relevant documents and training materials.

- FCPA training and awareness: Has the proposed third party received FCPA training? Are they TRACE certified or certified by some other recognizable entity?

One thing that you should keep in mind is that you will likely have pushback from your business team when it comes to making many of the inquiries listed above. However, my experience is that most proposed agents that have done business with US or UK companies have already gone through this process. Indeed, they understand that by providing this information in a timely manner they can set themselves apart as more attractive to international businesses.

The questionnaire fills several key roles in your overall management of third parties. Obviously, it provides key information that you need to know about who you are doing business with, and whether they have the capabilities to fulfill your commercial needs. Just as important is what is said if the questionnaire is not completed, or is only partially completed, such as lack of awareness of the FCPA, UK Bribery Act, or anti-corruption/anti-bribery programs generally. Lastly, the information provided (or not provided) in the questionnaire will assist you in determining what level of due diligence to perform.

Step 3: Due diligence

Most companies fully understand the need to comply with the FCPA regarding third parties as they represent the greatest risks for a FCPA violation. However, most companies are not created out of new cloth, but are ongoing enterprises with a fully up-and-running business in place. They need to bring resources to bear to comply with the FCPA while continuing to do business. This may be particularly true in the area of performing due diligence on third parties. Many companies understand the need for a robust third-party due diligence program, but have struggled with how to create an inventory to define the basis of risk for each foreign business partner, and thereby to perform the due diligence required under the FCPA.

Getting your arms around due diligence can sometimes seem bewildering for the compliance practitioner. However, the information that you should have developed in steps 1 and 2 of the lifecycle of third-party management should provide you with the initial information to consider the level of due diligence that you should perform on third parties.

Jay Martin, CCO at BakerHughes, often emphasizes that a company needs to evaluate and address its risks regarding third parties when he speaks on the topic. This means that an appropriate level of due diligence may vary depending on the risks arising from the particular relationship. So, for example, the appropriate level of due diligence required by a company when contracting for information technology services may be low, to reflect low risks of bribery on its behalf. Conversely, a business entering into the international energy market, and selecting an intermediary to assist in establishing a business in such markets, will typically require a much higher level of due diligence to mitigate the risks of bribery on its behalf.

Our British compliance cousins, of course, are subject to the UK Bribery Act. In the fourth of its six principles of an adequate procedures compliance program, the UK MOJ stated, "The commercial organisation applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery risks." The purpose of this principle is to encourage businesses to put in place due diligence procedures that adequately inform the application of proportionate measures designed to prevent persons associated with a company from bribing on their behalf. The MOJ recognizes that due diligence procedures act both as a procedure for anti-bribery risk assessment and as a risk-mitigation technique. The MOJ said that due diligence is so important that "the role of due diligence in bribery risk mitigation justifies its inclusion here as a Principle in its own right".

One question I am often asked is how to think through some of the relationships a company has with its various third parties in a manner to reasonably risk rank them. Initially, I would break things down into the sales side and the supply chain in order to begin any such analysis. Anecdotally, it is said that over 95 per cent of all FCPA enforcement actions involved third parties so this is one area where companies need to put in some thoughtful consideration. However, the key is that if you employ a "check-the-box" approach it may not only be inefficient, but more importantly *ineffective*. Because each compliance program should be tailored to an organization's specific needs, risks, and challenges, the information provided here should not be considered a substitute for a company's own assessment of the most appropriate corporate compliance program. In the end, if designed carefully, implemented earnestly, and enforced fairly, a company's compliance program – no matter how large or small the organization – will allow the company

generally to prevent violations, detect those that do occur, and remediate them promptly and appropriately.

Sales side

I tend to view things in a straightforward manner when it comes to representatives on the sales side of your business. I believe that any third-party representatives you have, whatever your might call them – sales reps, sales agents, commissioned sales agents, or anything else – should be viewed as high risk, and therefore they should receive your highest level of scrutiny. This is also true with any party which might be called, charitably or not, a "partner", whether that is a joint venture (JV) partner, plain old partner, teaming partner, or another monickered "partner". However, under this approach you should also consider the perception of corruption in the geographic area where you will use the third party. I recognize that you can overlay a financial threshold, but the reality is that if a sales representative generates such a small amount of money for your business you probably do not need them as representative.

At least with distributors, I have seen merit in more sophisticated approaches, such as that set out by David Simon, a partner at Foley and Lardner LLP, who advocates that risk analysis should more appropriately be based on the nature of a company's relationships with its distributors. The goal should be to determine which distributors are the most likely to qualify as agents, for whose acts the company would likely to be held responsible. He argues that it is a continuum of risk: on the low-risk end are distributors that are really nothing more than re-sellers with little actual affiliation with the supplier company; on the high-risk end are distributors who are very closely tied to the supplier company, who effectively represent the company in the market, and who end up looking more like a quasi-subsidiary than a customer.

Simon looks at agency principles to guide his analysis of whether a distributor qualifies as an agent for FCPA purposes. He argues that factors to consider include:

- The volume of sales made to the distributor;
- The percentage of total sales of the distributor's total business the principal's product represents;
- Whether the distributor represents the principal in the market, including whether it can (and does) use the company trademarks and logos in its business; and

- Whether the principal company is involved in the running of the distributor's business (such as by training the distributor's sales agents, imposing performance goals and objectives, or providing reimbursement for sales activity).

Once a company segregates the high-risk distributors that likely qualify as agents, and potentially subject the company to FCPA liability, from those that are mere resellers and pose less FCPA risk, FCPA compliance procedures can be tailored appropriately. For those distributors that qualify as "agents", and also pose FCPA risk, full FCPA due diligence, certifications, training, and contract language are imperative. For those that do not, more limited compliance measures that reflect the risk-adjusted potential liability are perfectly appropriate.

Supply chain

This determination of the level of due diligence and categorization of a supplier should depend on a variety of factors, including whether the supplier is:

- Located, or will operate, in a high-risk country;
- Associated with, or recommended or required by, a government official or his or her representative;
- Currently under investigation, the subject of criminal charges, or was recently convicted of criminal violations, including any form of corruption;
- A multinational publicly traded corporation with a recognized exemplary system of compliance and internal controls that has not been recently investigated or convicted of any corruption offense, or that has taken appropriate corrective action to remedy such conduct; or
- A provider of widely available services and products that are not industry specific, are offered to the public at large, and do not fall under the definition of minimal-risk supplier (as discussed below). You should note that any supplier with foreign government touch points should move up into the high level of scrutiny.

A high-risk supplier is an individual or an entity that is engaged to provide non-project-specific goods or services to a company. It presents a higher level of compliance risk because of the presence of one or more of the following factors:

- It is based or operates in a country that poses a high risk for corruption, money laundering, or commercial bribery;
- It supplies goods or services to a company from a high-risk country;
- It has a reputation in the business community for questionable business practices or ethics; or
- It has been convicted of, or is alleged to have been involved in, illegal conduct and has failed to undertake effective remedial actions.

Finally, it presents one or more of the following features, in which case the CCO should be consulted for further direction:

- It is located in a country that has inadequate regulatory oversight of its activities;
- It is in an unregulated business;
- Its ultimate or beneficial ownership is difficult to determine;
- The company has an annual spend of more than $100,000 with the supplier;
- It was established or registered in a jurisdiction where ownership is not transparent, or where ownership is permitted in the form of bearer shares;
- It is registered or conducts business in a jurisdiction that does not have anti-corruption, anti-money laundering (AML), and anti-terrorism laws comparable to those of the US and UK; or
- It lacks a discernable and substantial business history.

A low-risk supplier is an individual or a non-publicly held entity that conducts business, such as a sole proprietorship, partnership, or privately held corporation, located in a low-risk country. Some indicia include:

- That it supplies goods, equipment, or services directly to a company in a low-risk country;
- The company has an annual spend of less than $100,000 with the supplier; and
- The supplier is not involvement with any foreign government, government entity, or government official.

However, a supplier may be considered a low risk where it is subject to the highest disclosure and auditing and reporting standards, such as those

companies publicly traded on a reputable and highly regulated stock exchange, such as the New York or London exchanges.

Below the high and low risk categories, I would add two other categories of suppliers which present very low compliance risks. The first is "minimal-risk suppliers", which generally provide to a company goods and services that are non-specific to a particular project and the value of the transaction is $25,000 or less. Some examples might be the routine supply of fungible items and services, including, among others: office supplies, such as paper, furniture, computers, copiers, and printers; industrial or factory supplies, including cleaning materials, solvents, safety clothing, and off-the-shelf equipment and parts; crating and other standard materials for packing products for shipping; leasing and rental of company cars and other equipment; and airline or other travel tickets or services. It may also include legal services from professional firms that are approved and overseen by a company's legal department; investigative services from professional firms that are approved and overseen by a legal department and that do not interact with government agencies on behalf of a company; and accounting and financial services from professional firms that are approved and overseen by a company finance department or audit committees, and that do not interact with government agencies on behalf of a company.

Finally, is the category of third parties that provide widely available services and products that are not industry specific, are offered to the public at large, and do not fall under the definition of minimal-risk supplier. These include, among others, wide circulation newspapers, magazines, florists, daily limousine and taxi, airline, and food delivery (including coffee shops, pizza parlors, and take out) services. These third parties raise even less than minimal risk to a company, especially when their services and products are provided in a non-high risk country. Suppliers in this category require no FCPA due diligence.

OCEG president Carol Switzer, writing in *Compliance Week*, suggested that you should initially set up categories for your third parties of high, moderate, and low risk. Based upon which risk category the third party falls into, you can design specific due diligence. She defined low-risk screening as "trusted data source search and risk screening such as… World Compliance"; moderate risk screening as "enhanced evaluation to include in-country public records… and research into corporate relationships"; and high risk screening as basically a "deep dive assessment" where there is an audit/review of third-

party controls and financial records and in-country interviews and investigations "leveraging local data sources".

A three-step approach was also discussed favorably in the DOJ's Opinion Procedure Release, number 10-02. In this release, the DOJ discussed the due diligence performed by the requesting entity: "First, [the requestor, a Eurasian subsidiary] conducted an initial screening of six potential grant recipients by obtaining publicly available information and information from third-party sources… Second, the Eurasian Subsidiary undertook further due diligence on the remaining three potential grant recipients. This due diligence was designed to learn about each organization's ownership, management structure and operations; it involved requesting and reviewing key operating and assessment documents for each organization, as well as conducting interviews with representatives of each MFI to ask questions about each organization's relationships with the government and to elicit information about potential corruption risk. As a third round of due diligence, the Eurasian Subsidiary undertook targeted due diligence on the remaining potential grant recipient, the Local MFI. This diligence was designed to identify any ties to specific government officials, determine whether the organization had faced any criminal prosecutions or investigations, and assess the organization's reputation for integrity."[4]

Based on the wisdom of the aforementioned compliance experts, Opinion Release 10-02 and others I have broken due diligence down into three stages: Level I, Level II, and Level III. A very good description of the three levels of due diligence was presented by Candace Tal, Founder and CEO of Infortal.[5]

Level I

First-level due diligence typically consists of checking individual names and company names through several hundred global watch lists, comprised of AML, anti-bribery, and sanctions lists, coupled with other financial corruption and criminal databases. These global lists create a useful first-level screening tool to detect potential red flags for corrupt activities. It is also a very inexpensive first step in compliance from an investigative viewpoint. Tal believes that this basic, Level I due diligence is extremely important for companies to complement their compliance policies and procedures, demonstrating a broad intent to actively comply with international regulatory requirements.

Level II

Level II due diligence involves supplementing Level I due diligence with a deeper screening of international media, typically the major newspapers and periodicals from all countries, plus detailed internet searches. Such inquiries will often reveal other forms of corruption-related information, and may expose undisclosed or hidden information about the company, the third party's key executives, and associated parties. I believe that Level II should also include an in-country database search regarding the third party. Some other types of information that you should consider obtaining are country of domicile and international government records; use of in-country sources to provide assessments of the third party; and a check for international derogatory electronic and physical media searches. You should perform both English and foreign-language repositories searches on the third party in its country of domicile, and, if you are in a specific industry, you should use technical specialists to obtain information from sector-specific sources.

Level III

This level is the "deep dive". It will require an in-country "boots on the ground" investigation. I agree with Tal that a Level III due diligence investigation is designed to supply your company "with a comprehensive analysis of all available public records data supplemented with detailed field intelligence to identify known and more importantly unknown conditions. Seasoned investigators who know the local language and are familiar with local politics bring an extra layer of depth assessment to an in country investigation." Further, "Direction of the work and analyzing the resulting data is often critical to a successful outcome; and key to understanding the results both from a technical perspective and understanding what the results mean in plain English. Investigative reports should include actionable recommendations based on clearly defined assumptions or preferably well-developed factual data points."

More than simply an investigation of the company, critically, Level III due diligence should also include a site visit, coupled with onsite interviews. Tal says that some other things you should investigate will include "an in-depth background check of key executives or principal players. These are not routine employment-type background checks, which are simply designed to confirm existing information, but rather executive due diligence checks designed to investigate hidden, secret or undisclosed information about that individual." Tal

believes that such "[r]eputational information, involvement in other businesses, direct or indirect involvement in other law suits, history of litigious and other lifestyle behaviors which can adversely affect your business, and public perceptions of impropriety, should be disclosed publically."

Further, you may need to engage a foreign law firm to investigate the third party in its home country to determine its compliance with its home country's laws, licensing requirements, and regulations. Lastly, and perhaps most importantly, you should use Level III to look the proposed third party in the eye and get a firm idea of his or her cooperation and attitude towards compliance; one of the most important inquiries is not legal, but based upon the response and cooperation of the third party. More than simply trying to determine if the third party objected to any portion of the due diligence process, or to the scope, coverage, or purpose of the FCPA, you can use the third-level due diligence to determine if the third party is willing to stand up under the FCPA, and whether you are willing to partner with the third party.

The Risk Advisory Group created a handy chart of its Level I, II, and III approaches to integrity and due diligence, reproduced overleaf. I have found it useful in explaining the different scopes and focuses of the various levels of due diligence.

There are many different approaches to the specifics of due diligence. By laying out some of the approaches favored by other experts in the field, I hope to encourage you can craft the relevant portions into your program. The Level I, II, and III trichotomy appears to have found the greatest favor, and is a process that you should be able to implement in a straightforward manner. However, as Jay Martin constantly says, you need to assess your company's own risk and manage that risk. So, if you need to perform additional due diligence to answer questions or clear red flags, you should do so.

Level	Issues addressed	Scope of investigation
I	That the company exists; Identities of directors and shareholders; Whether such persons are on regulators' watch lists; Signs that such persons are government officials; Obvious signs of financial difficulty; Signs of involvement in litigation; and Media reports linking the company to corruption.	Company registration and status; Registered address; Regulators' watch lists; Credit checks; Bankruptcy/liquidation proceedings; Review of accounts and auditors comments; Litigation search; and Negative media search.
II	As above, with the following additions: Public profile integrity checks; Signs of official investigations and/or sanctions from regulatory authorities; and Other anti-corruption red flags.	As above with the following additions: Review and summarize all media and internet references; Review and summarize relevant corporate records and litigation filings, including local archives; and Analyze and cross-reference all findings.
III	As above, with the following additions: Seeking fuller answers to any questions raised by drawing on a wider range of intelligence sources and/or addressing specific issues of potential concern already identified.	As above with the following additions: Inquiries via local sources; Inquiries via industry experts; Inquiries via western agencies, such as embassies or trade promotion bodies; and Inquires via sources close to local regulatory agencies.

Table 1: Level I, II, and III approaches to integrity and due diligence.

Step 4: The contract

Next up is step 4: the contract. However, before we get to the contracting stage, a word about what to do with steps 1-3. You cannot simply obtain the information detailed in these first three steps, you must evaluate the information and show that you have used it in your process. If it is incomplete, it must be completed. If red flags have appeared, these red flags must be cleared or you must demonstrate how you will manage the risks identified. In others words, you must document, document, and document that you have read, synthesized, and evaluated the information garnered in steps 1–3. As the DOJ and SEC continually remind us, a compliance program must be a living, evolving system, and not simply a "check-the-box" exercise.

After you have completed steps 1–3 and then evaluated and documented your evaluation, you are ready to move onto to step 4: the contract. Obviously, any commercial relationship should be governed by the terms and conditions of a written contract. Clearly, your commercial terms should be set out in the contract. On the subject of commercial terms, the FCPA Guidance intones "Additional considerations include payment terms and how those payment terms compare to typical terms in that industry and country, as well as the timing of the third party's introduction to the business." This means that you need to understand what the rate of commission is, and whether it is reasonable for the services delivered. If the rate is too high, this could be indicative of corruption, as high commission rates can create a pool of money to be used to pay bribes. If your company uses a distributor model in its sales side, then it needs to review the discount rates it provides to its distributors to ascertain that the discount rate is warranted.

In a presentation at the 2014 SCCE Utility and Energy Conference, Flora Francis and Andrew Baird of GE Oil & Gas described the process by which GE reviews the risks around each third party with which it does business. Initially, both speakers made clear that GE's program was the company's response to its own assessed risks. Further, the compliance program has evolved, not only as the company's risks have evolved, but also as the company has determined what works and does not work so well. Within the realm of third parties, the prescient question from compliance to the business unit would be "what is your go-to-market strategy?" And "how will your use of third parties assist you in carrying out that strategy?" Some of the factors the speakers cited include your company's market coverage strategy, product segmentation, pricing and margin expectation, an added capability which

your company may not possess, such as technology, and finally local legal requirements.

Some of the factors GE considers when evaluating a third party include the following:

- Business model: Do we need third parties to reach our customers or can we build the organization ourselves?
- In-house capabilities: Do we already have the organization in place to handle these capabilities?
- Overlap: Do we already have a third party in the region/country that can handle our needs?
- Volume of business: How much business will this third party bring to the company?
- Compliance risk: Where is the third party located? Will they interact with government officials? Do they have same commitment to compliance?
- Regulatory environment: Is it simple or strict? What are the chances of regulatory violations?
- Reputation: What is the third party's reputation in the market?

GE takes this information and then breaks downs the risks into low risk and high risk. A low risk receives a limited review and analysis, while a high risk receives an escalated review and analysis consisting of the following: compliance, legal, business leadership, and finance.

More than simply the level of review, I was interested in the "risk score drivers" that GE has developed. Once again, the speakers emphasized that these are GE's risk score drivers and have been developed over time through the company's internal analysis and processes. Nevertheless, I found them to be a very useful way to think about third-party risk. The risk score drivers listed were:

- Country the third party is located in, or which it sells into;
- Experience by the third party with the sales channel;
- Type of third party involved: agent, reseller, distributor;
- Commission rate (is it standard or non-standard?);
- Will any sub-third party relationships be involved;
- Will the third party sell to government entity or instrumentality;
- Do any of the third party's principals, officers, or agents work for a foreign government, state owned enterprise, or political party;

- Was the third party mandated by customer or the end user;
- What is the third party's contract duration;
- Is the third party involved in more than one project;
- Does the third party have any historical compliance issues;
- What is the percent of sales with products or services; and
- What is GE's annual revenue with the third party?

GE compliance then takes these scoring factors and puts them into an evaluation matrix when determining the amount of risk involved and whether or not the company should move forward with a proposed third party.

In addition to the above analysis from the compliance perspective, you should also incorporate compliance terms and conditions into your contracts with third parties. I would suggest that you begin with some type of compliance terms and conditions template, which can be used as a starting point for your negotiations. The advantages of such a template are several. They include:

1. The contract language is tested against real events;
2. The contract language assists the company in managing its compliance risks;
3. The contract language fits into a series of related contracts;
4. The contract language is straightforward to administer; and
5. The contract language helps to manage the expectations of both contracting parties regarding anti-bribery and anti-corruption.

What are the compliance terms and conditions that you should include in your commercial contracts with third parties? In the Panalpina deferred prosecution agreement (DPA), Attachment C, Section 12, is found the following language: "Where necessary and appropriate, Panalpina will include standard provisions in agreements, contracts, and renewals thereof with all agents and business partners that are reasonably calculated to prevent violations of the anticorruption laws, which may, depending upon the circumstances, include: (a) anticorruption representations and undertakings relating to compliance with the anticorruption laws; (b) rights to conduct audits of the books and records of the agent or business partner to ensure compliance with the foregoing; and (c) rights to terminate an agent or business partner as a result of any breach of anti-corruption laws, and regulations or representations and undertakings related to such matters."

In the Johnson & Johnson (J&J) DPA, the same language as is used in the Panalpina DPA is found in Attachment C, entitled "Corporate Compliance Program". However, in Attachment D, entitled "Enhanced Compliance Obligations", the following language is found: "Contracts with such third parties are to include appropriate FCPA compliance terms and conditions including: (i) representatives and undertakings of the third party to compliance; (ii) right to audit; and (iii) right to terminate."

Mary Jones suggested the following language be present in your compliance terms and conditions:[6]

- Payment mechanisms that comply with this manual, the FCPA, the UK Bribery Act, and other applicable anti-corruption and/or anti-bribery laws during the term of such a contract;
- The counterparty's obligation to maintain accurate books and records in compliance with the company's policy and compliance manual;
- The counterparty's obligation to certify on an annual basis that:
  - Counterparty has not made, offered, or promised any payment or gift of money or anything of value, directly or indirectly, to any government official (or any other person or entity if UK Bribery Act applies) for the purpose of obtaining or retaining business or getting any improper business advantage; and
  - Counterparty has not engaged in any conduct or behavior prohibited by the code of conduct, anti-corruption policy, and compliance manual and other applicable anti-corruption and/or anti-bribery law;
- The company's right to audit the counterparty's books and records, including, without limitation, any documentation relating to the counterparty's interaction with any governmental entity (or any entity if UK Bribery Act applies) on behalf of the company, and the counterparty's obligation to cooperate fully with any such audit; and
- Remedies (including termination rights) for the failure of the counterparty to comply with the terms of the contract, the code of conduct, the anti-corruption policy and compliance manual, and other applicable anti-corruption and/or anti-bribery law during the term of such contract.

Based on the foregoing experts and the research I have engaged in, I believe that compliance terms and conditions should be stated directly in the document, whether such document is a simple agency or consulting agreement or a JV

with several formation documents. The compliance terms and conditions should include representations that in all undertakings the third party will make no payments of money, or anything of value, nor will such be offered, promised, or paid, directly or indirectly, to any foreign officials, political parties, party officials, or candidates for public or political party office, to influence the acts of such officials, political parties, party officials, or candidates in their official capacity, to induce them to use their influence with a government to obtain or retain business, or to gain an improper advantage in connection with any business venture or contract in which the company is a participant.

In addition to the above affirmative statements regarding conduct, a commercial contract with a third party should include the following compliance terms and conditions:

- Indemnification: Full indemnification for any FCPA violation, including all costs for the underlying investigation.
- Cooperation: Require full cooperation with any ethics and compliance investigation, specifically including the review of foreign business partner emails and bank accounts relating to your company's use of the foreign business partner.
- Material breach of contract: Any FCPA violation is made a material breach of contract, with no notice and opportunity to cure. Further, such a finding will be the grounds for immediate cessation of all payments.
- No sub-vendors (without approval): The foreign business partner must agree that it will not hire an agent, subcontractor, or consultant without the company's prior written consent (to be based on adequate due diligence).
- Audit rights: An additional key element of a contract between a US company and a foreign business partner should include the retention of audit rights. These audit rights must exceed the simple audit rights associated with the financial relationship between the parties and must allow a full review of all FCPA-related compliance procedures, such as those for meeting with foreign governmental officials and compliance-related training.
- Acknowledgment: The foreign business partner should specifically acknowledge the applicability of the FCPA to the business relationship, as well as any country or regional anti-corruption or anti-bribery laws which apply to either the foreign business partner or business relationship.

- Ongoing training: Require that the top management of the foreign business partner and all persons performing services on your behalf shall receive FCPA compliance training.
- Annual certification: Require an annual certification stating that the foreign business partner has not engaged in any conduct that violates the FCPA or any applicable laws, nor is it aware of any such conduct.
- Re-qualification: Require the foreign business partner re-qualify as a business partner at a regular interval of no greater than every three years.

Many will exclaim, "What an order, I can't go through with it." By this they mean that they do not believe that they will be able to get the third party to agree to such compliance terms and conditions. I have found that, while it may not be easy, it is relatively simple to get a third party to agree to these, or similar, terms and conditions. One approach to take is to make the terms and conditions non-negotiable. When faced with such a position on non-commercial terms, many third parties will not put up a fight. There is some flexibility, but the DOJ will require the minimum terms and conditions that it has suggested in the various Attachment Cs to the DPAs, as previously discussed. However, the best argument I have found is that, if a third party agrees with these terms and conditions, they can then use that as a market differentiator from other third parties who have not gone through the lifecycle management of a third party as this series has discussed.

Step 5: Management of the relationship

I often say that after you complete steps 1–4 in the lifecycle management of a third party, the real work begins. That work is found in step 5: the management of the relationship. While the work done in steps 1–4 is absolutely critical, if you do not manage the relationship it can all go downhill very quickly and you might find yourself with a potential FCPA or UK Bribery Act violation. There are several different ways that you should manage your post-contract relationship. Here we will explore some of the tools you can use to help make sure that all the work you have done in steps 1–4 will not be for nothing, and that you will have a compliant anti-corruption relationship with your third party going forward.

Managing third-party relationships is an area that continues to give companies trouble and heartburn. The "2013 Anti-Bribery and Corruption Benchmarking Report" by Kroll and *Compliance Week* found that many

companies are still struggling with ongoing anti-corruption monitoring and training for their third parties.[7] Regarding training, 47 per cent of the respondents said that they conduct no anti-corruption training with their third parties at all. The efforts companies do take to educate and monitor third parties are somewhat pro forma. More than 70 per cent require certification from their third parties that they have completed anti-corruption training; 43 per cent require in-person training; and another 40 per cent require online training. Large companies require training considerably more often than smaller ones, although when looking at all the common training methods, 100 per cent of respondents say their company uses at least one method, if not more.

While the FCPA Guidance itself only provides that "companies should undertake some form of ongoing monitoring of third-party relationships". Diana Lutz, writing in a white paper by The Steele Foundation entitled "Global anti-corruption and anti-bribery program best practices", said: "As an additional means of prevention and detection of wrongdoing, an experienced compliance and audit team must be actively engaged in home office and field activities to ensure that financial controls and policy provisions are routinely complied with and that remedial measures for violations or gaps are tracked, implemented and rechecked."[8]

Another noted commentator has discussed techniques to provide this management and oversight to any third-party relationship. Carol Switzer, writing in *Compliance Week* magazine, set out a five-step process for managing corruption risks, which I have adapted for third parties:

1. Screen: Monitor third-party records against trusted data sources for red flags;
2. Identify: Establish help lines and other open channels for reporting of issues and asking compliance-related questions by third parties;
3. Investigate: Use appropriately qualified investigative teams to obtain and assess information about suspected violations;
4. Analyze: Evaluate data to determine "concerns and potential problems" by using data analytics, tools, and reporting; and
5. Audit: Finally, your company should have regular internal audit reviews and inspections of the third party's anti-corruption program, including testing and assessment of internal controls to determine if enhancement or modification is necessary.

Based upon the foregoing and other commentators, I believe there are several different roles in a company that play a function in the ongoing monitoring of the third party. While there is overlap, I believe that each role fulfills a critical function in any best practices compliance program.

Relationship manager

There should be a relationship manager for every third party with which your company does business. The relationship manager should be a business unit employee who is responsible for monitoring, maintaining, and continuously evaluating the relationship between your company and the third party. Some of the duties of the relationship manager may include:

- Point of contact with the third party for all compliance issues;
- Maintaining periodic contact with the third party;
- Meeting annually with the third party to review its satisfaction of all company compliance obligations;
- Submitting annual reports to the company's oversight committee, summarizing services provided by the third party;
- Assisting the company's oversight committee with any issues with respect to the third party.

Compliance professional

Just as a company needs a subject matter expert (SME) in anti-bribery compliance to be able to work with the business folks and answer the usual questions that come up in the day-to-day routine of doing business internationally, third parties also need such access. A third party may not be large enough to have its own compliance staff, so I advocate a company providing such a dedicated resource to third parties. I do not believe that this will create a conflict of interest or that there are other legal impediments to providing such services. They can also include anti-corruption training for the third party, either through onsite or remote mechanisms. The compliance practitioner should work closely with the relationship manager to provide advice, training, and communications to the third party.

Oversight committee

I advocate that a company should have an oversight committee review all documents relating to the full panoply of a third party's relationship with the

company. It can be a formal structure or some other type of group but the key is to have the senior management put a "second set of eyes" on any third parties who might represent a company in the sales side. In addition to the basic concept of process validation of your management of third parties, as third parties are recognized as the highest risk in FCPA or Bribery Act compliance, this is a manner to deliver additional management of that risk.

After the commercial relationship has begun, the oversight committee should monitor the third-party relationship on no less than an annual basis. This annual audit should include a review of remedial due diligence investigations and evaluation of any new or supplementary risk associated with any negative information discovered from a review of financial audit reports on the third party. The oversight committee should review any reports of any material breach of contract, including any breach of the requirements of the company code of ethics and compliance. In addition to the above remedial review, the oversight committee should review all payments requested by the third party to assure such payment is within the company guidelines and is warranted by the contractual relationship with the third party. Lastly, the oversight committee should review any request to provide the third party with any type of non-monetary compensation, and, as appropriate, approve such requests.

Audit

A key tool in managing the relationship with a third party post-contract is auditing the relationship. I hope that you will have secured audit rights, as that is an important clause in any compliance terms and conditions. Your audit should be a systematic, independent, and documented process for obtaining evidence and evaluating it objectively to determine the extent to which your compliance terms and conditions are followed. Noted fraud examiner expert Tracy Coenen described the process as one to (1) capture the data; (2) analyze the data; and (3) report on the data. This is also appropriate for a compliance audit. As a baseline, I would suggest that any audit of a third party include, at a minimum, a review of the following:

- The effectiveness of existing compliance programs and codes of conduct;
- The origin and legitimacy of any funds paid to company;
- Books, records, and accounts of the company or those of any of its subsidiaries, joint ventures, or affiliates related to work performed for, or services or equipment provided to, the company;

- All disbursements made for or on behalf of the company; and
- All funds received from the company in connection with work performed for, or services or equipment provided to, the company.

If you want to engage in a "deeper dive", you might consider evaluation of some of the following areas:

- Review of contracts with third parties to confirm that the appropriate FCPA compliance terms and conditions are in place.
- Determine that actual due diligence took place on the third party.
- Review FCPA compliance training program – both the substance of the program and attendance records.
- Does the third party have a hotline or any other reporting mechanism for allegations of compliance violations?
- If so how are such reports maintained? Review any reports of compliance violations or issues that arose through anonymous reporting, hotline, or any other reporting mechanism.
- Does the third party have written employee discipline procedures? If so, have any employees been disciplined for any compliance violations? If yes, review all relevant files relating to any such violations to determine the process used and the outcome reached.
- Review employee expense reports for employees in high-risk positions or high-risk countries.
- Testing for gifts, travel, and entertainment that were provided to, or for, foreign governmental officials.
- Review the overall structure of the third party's compliance program. If the company has a designated compliance officer to whom, and how, does that compliance officer report?
- How is the third party's compliance program designed to identify risks and what has been the result of any so identified?
- Review a sample of employee commission payments and determine if they follow the internal policy and procedure of the third party.
- With regard to any petty cash activity in foreign locations, review a sample of activity and apply analytical procedures and testing. Analyze the general ledger for high-risk transactions and cash advances and apply analytical procedures and testing.

In addition to monitoring and oversight of your third parties, you should periodically review the health of your third party management program. Once again I turn to Diana Lutz and her colleague Marjorie Doyle and their white paper on third parties, in which they gave a checklist to test companies on their relationships with their third parties:[9]

1. Do you have a list or database of all your third parties and their information?
2. Have you done a risk assessment of your third parties and prioritized them by level of risk?
3. Do you have a due diligence process for the selection of third parties, based on the risk assessment?
4. Once the risk categories have been determined, create a written due diligence process.
5. Once the third party has been selected based on the due diligence process, do you have a contract with the third party stating all the expectations?
6. Is there someone in your organization who is responsible for the management of each of your third parties?
7. What are "red flags" regarding a third party?

Perhaps now you will understand why I say that after you prepare the business justification; send out, receive back, and evaluate the questionnaire; set the appropriate level of due diligence; evaluate the due diligence and execute a contract with appropriate compliance terms and conditions; it is now that the real work begins, as you have to manage the third party relationship.

Some final thoughts

In my writing, I often cite Paul McNulty, chair of the Global Corporate Compliance steering committee at Baker & McKenzie LLP, who often talks about the three areas of inquiry he would assess regarding an FCPA enforcement action or what I call "McNulty's maxims":

- Maxim No. 1: "What did you do to stay out of trouble?"
- Maxim No. 2: "What did you do when you found out?" and
- Maxim No. 3: "What remedial action did you take?"

He also continually emphasizes that, as a key component, a company must document its overall compliance efforts. His Baker & McKenzie partner Stephen Martin, believes that one key indication of a best practices compliance program is the ability of a company to respond to an inquiry by a regulator. Martin points out to do so a company must document what it does for its compliance efforts on an ongoing basis. However, more important than simply the ability to document the results of your company's compliance efforts is the ability of a company to quickly and efficiently respond to a prosecutor's request for information in a timely manner.

McNulty's maxims and the regulators' eyes lead me to continually give my mantra of FCPA compliance, which is document, document, and document. Each of the steps you take in the management of your third parties must be documented. Not only must they be documented, but they must be stored and managed in a manner that you can retrieve them with relative ease. At one company I worked at, when the assignment was initially given to the in-house counsel, similar to the one who started this discussion, it took the company over six months to come up with a spreadsheet to simply list the third-party representatives in the sales chain. At another company I worked at, it took almost one month to get a computer-generated list of the vendors in the supply chain. The days of such delays are long gone. So you have to be organized in your documentation and have the ability to retrieve information in a reasonable fashion.

The management of third parties is absolutely critical in any best practices compliance program. As you sit at your desk pondering whether this assignment given to you by the CCO is a career-ending dead-end, you should take heart, because there is clear and substantive guidance out there which you can draw upon.

References

1. Kroll, K., "How Tyco Turned Around Third-Party Risk Program", Compliance Week, September 2011.
2. Cassin, R. L., "Compliance Officers Troubled By Third-Party Risk", The FCPA Blog, 6 June 2012, see www.fcpablog.com/blog/2012/6/6/compliance-officers-troubled-by-third-party-risk.html.
3. Randy Colrey, executive vice president (EVP) and global compliance officer at Edelmen Inc., in a presentation at Compliance Week 2012, entitled "3rd Party Due Diligence Best Practices in Establishing an Effective Anti-Corruption Program", 2012.

4. FCPA Opinion Procedure Release 10-02, 16 July 2010, see www.justice.gov/criminal/fraud/fcpa/opinion/2010/1002.pdf.
5. Tal, C., "Deep Level Due Diligence: What You Need to Know", FCPA Compliance and Ethics Blog, 7 November 2012, see tfoxlaw.wordpress.com/2012/11/07/deep-level-due-diligence-what-you-need-to-know.
6. Jones, M., "Panalpina's World Wide Web", FCPA Compliance and Ethics Blog, 12 November 2012, see tfoxlaw.wordpress.com/2012/11/12/panalpina-s-world-wide-web.
7. Kroll and Compliance Week, "2013 Anti-Bribery and Corruption Benchmarking Report – A joint effort between Kroll and Compliance Week", 2013.
8. Lutz, D., "Global anti-corruption and anti-bribery program best practices", white paper, The Steele Foundation.
9. Ibid.

Chapter 8: How do I love thee – Confidential reporting and internal investigations

THE FCPA Guidance provides a clear and concise statement about hotlines: "An effective compliance program should include a mechanism for an organization's employees and others to report suspected or actual misconduct or violations of the company's policies on a confidential basis and without fear of retaliation." More than simply making hotlines available, however, companies also have to make real efforts to *listen* to employees. Mike Volkov has stated, "Companies have to spend time addressing this issue. The issue can be handled with several strategies: (1) managers have to be specifically trained on how to handle employee concerns; (2) managers have to be given real performance incentives on this issue as part of their evaluations; (3) company officials have to devote communications resources to reinforcing the company's culture and values to create an environment and expectation that managers will raise employee concerns."[1]

The reason is that its employees are a company's best source of information about what is going on at the company. It is certainly a best practice for a company to listen to its own employees, particularly to help improve its processes and procedures. But more than listening to its employees, a company should also provide a safe and secure route for employees to communicate their concerns. This is the underlying rationale behind an anonymous reporting system within any organization. Both the US Sentencing Guidelines and the OCED Good Practices list as one of their components an anonymous reporting mechanism by which employees can report compliance and ethics violations. Of course, the Dodd-Frank whistleblower provisions also give companies an incentive to implement an internal hotline.

What are some of the best practices for a hotline? I would suggest that you start with at least the following:

1. Availability: A hotline should be available 24 hours a day, 7 days a week, and toll-free. It should be available in the native tongue of the person utilizing it so if your work force uses more than one language for inter-company communications, your hotline should reflect this as well.
2. Anonymity: While some foreign jurisdictions do not allow anonymous reporting, the US is not one of them. You need to have a mechanism that allows an employee to make an anonymous report and put in safeguards which will ensure anonymity going forward should the reporting employee desire it.
3. Escalation: After a report is received through the hotline it should be distributed to the appropriate person or department for action and oversight. This would also include resolution of the information presented, if warranted, and consistent application of the investigation process throughout the pendency of the matter.
4. Follow-up: There should be a mechanism for follow-up with the hotline reporter, even if the report is made anonymously. This allows the appropriate person within your organization to substantiate the report or obtain additional information at an early stage, if appropriate.
5. Oversight: The information communicated through the hotline should be available to the appropriate board committee or management committee in the form of statistical summaries and an audit trail should be available to the appropriate oversight group of actions taken and resolution of any information reported through the hotline.

The hotline can be a key company tool in an effective FCPA compliance program. Properly advertised and then utilized, it can assist a company to learn about issues and take appropriate actions before these issues erupt into more serious problems. Lastly, the proper maintenance of a hotline will not only allow a company to track compliance issues as they come into the system and document its response, but also to use this information as an ongoing audit of its FCPA compliance system.

Is your hotline working for you? José Tabuena, writing in *Compliance Week*, shared a case study, which provided three lessons regarding hotlines:[2]

- First, a helpline is of no value if the workforce is not aware of it. Although a helpline was in place, it became apparent that a segment of the company had not been informed. It was hotline data that revealed this gap. By

reviewing data segmented by region, department, incident classification, and other criteria, it became obvious in comparison to the rest of the organization that the IT department had not used the helpline.

- Second, the ethics and compliance office obtained support from the chief information officer (CIO) for making IT part of the helpline community and for designating a liaison within the IT function. The support of department leadership likely influenced the success of the training and communications delivered by the ethics and compliance staff.
- Third, the awareness of the helpline is not sufficient to ensure success. The company made sure that issues and allegations were addressed and investigated, as needed. Employees who choose not to report wrongdoing indicate a belief that nothing will be done anyway, so why take the risk? Employees also cite fear of retaliation as a reason for not reporting.

A company hotline or other internal reporting mechanism can help to establish the credibility of the helpline as a resource to raise issues and report misconduct. Equally importantly, the helpline proved to be a successful management tool.

How does your organization treat whistleblowers?

While I would hope that most US and European companies have moved past the situation where whistleblowers are ostracized, or worse threatened, one can certainly remember the GlaxoSmithKline PLC (GSK) whistleblower Cheryl Eckard. In a 2010 article in the *Guardian*, Graeme Wearden reported that Eckard was fired by the company "after repeatedly complaining to GSK's management that some drugs made at Cidra were being produced in a non-sterile environment, that the factory's water system was contaminated with micro-organisms, and that other medicines were being made in the wrong doses."[3] She later was awarded $96 million as her share of the settlement of a Federal Claims Act whistleblower lawsuit. Eckard was quoted as saying, "It's difficult to survive this financially, emotionally, you lose all your friends, because all your friends are people you have at work. You really do have to understand that it's a very difficult process but very well worth it."

More recently, the example of NCR Corp., was cited in the *Wall Street Journal* by Christopher M. Matthews and Samuel Rubenfeld.[4] According to the article, NCR spokesperson Lou Casale said "While NCR has certain concerns about the veracity and accuracy of the allegations, NCR takes allegations

of this sort very seriously and promptly began an internal investigation that is ongoing" regarding whistleblowers' claims of FCPA violations. In a later *Wall Street Journal* article, Matthews reported that NCR also said that the company "has certain concerns about the motivation of the purported whistleblower and the accuracy of the allegations it received, some of which appear to be untrue."[5]

Lastly, the situation of two whistleblowers from the British company EADS was reported by Carola Hoyos in the *Financial Times*.[6] Hoyos told the story of two men who notified company officials of allegations of bribery and corruption at the company and suffered for their actions. The first, Mike Paterson, then financial controller for an EADS subsidiary GPT, internally reported "unexplained payments to the Cayman Island bank accounts for Simec International and Duranton International, which totaled £11.5M between 2007 and 2009". Hoyos reported that Paterson was so marginalized in his job that he was basically twiddling his thumbs all day at work.

The second whistleblower was Ian Foxley, a retired British lieutenant-colonel, who had joined the company in the spring of 2010 and had been stationed in Saudi Arabia to oversee a £2 million contract between the British Ministry of Defence and the Saudi Arabian National Guard. In December 2010, Foxley discovered some of the concerns which Mike Paterson had raised. According to Hoyos, "The morning after he discovered Mr. Paterson's concerns he assessed the emails that Mr. Paterson had told him he had written over the previous three years." This led Foxley to flee Saudi Arabia with documents of these suspicious payments, which he has turned over to the Institute of Chartered Accountants and the UK Serious Fraud Office (SFO).

What does the response of any of these three companies say about the way that they treat whistleblowers? While I doubt that many companies will ever come to embrace whistleblowers, they must embrace the FCPA Guidance language. However, it is worth noting that by marginalizing, attacking, or even making a whistleblower fear for their life, companies can drive whistleblowers to go the DOJ, SEC, or SFO. The FCPA Guidance recognized that "[a]ssistance and information from a whistleblower who knows of possible securities law violations can be among the most powerful weapons in the law enforcement arsenal".

A recent white paper on whistleblowing, released by the Ethics Resource Center (ERC), detailed several findings that the ERC had determined through surveys, interviews, and dialogues.[7] One of the

key findings was that a culture of ethics within a company *does matter*. Such a culture should start with a strong commitment to ethics at the top; however, it is also clear that this message must be reinforced throughout all levels of management, and that employees must understand that their company has the expectation that ethical standards are maintained as vital components of the business's day-to-day operations. If employees have this understanding, they are more likely to conduct themselves with integrity and report misconduct by others. Additionally, those employees who report misconduct are often motivated by the belief that their reports will be properly investigated. Conversely, most employees are less concerned with the particular outcome than in knowing that their report was seriously considered. This is the "fair process doctrine" in action. Adhering to the fair process doctrine in your compliance program is critical for you, as a compliance specialist or for your compliance department to have credibility with the rest of the workforce.

To reiterate, when it comes to internal company investigations, if your employees do not believe that the investigation is fair and impartial, then it is *not fair and impartial*. Furthermore, those involved must have confidence that any internal investigation is treated seriously and objectively. One of the key reasons that employees will go outside of a company's internal hotline process is because they do not believe that the process will be fair.

Phrasing it in another way, Mike Volkov had these suggestions:[8]

1. Listen to the whistleblower: In dealing with a whistleblower, it is critical to listen to the whistleblowers' concerns;
2. Do not "overpromise": At the conclusion of an initial meeting with a whistleblower, the company representative should inform the whistleblower that the company will review the allegations, conduct a "preliminary" investigation, and report back to the whistleblower during, or at the conclusion of, any investigation;
3. Conduct a fair investigation: Depending on the nature of the allegations, a follow-up inquiry should be conducted.

The steps taken in the investigation should be *documented*. I would emphasize, yet again, that after your investigation is complete, the fair process doctrine demands that any discipline must not only be administered fairly but it must be administered uniformly across the company for a violation of any compliance policy.

What is your FCPA investigation protocol?

Jackie Trevino, senior manager, corporate compliance at Fluor Corporation, presented her company's investigative protocol at a SCCE National Conference. It is an excellent place to start when considering the creation of your own program. Fluor's five steps are as follows:

Step 1: Opening and categorizing the case

Under this first step, you should categorize the ethics and compliance violation. You should notify the relevant individuals, including those on your investigation team and any senior management members under your notification protocols. After notification, you should assemble your investigation team for preliminary meetings and assessments. This step should be accomplished in one to three days after the allegation comes in to compliance, either through your reporting structure or other means.

Step 2: Planning the investigation

After assembling your investigation team, you should determine the required investigation tasks. These would include document review and interviews. If hard drives need to be copied or documents put on hold or sequestered in any way, or relationships need to be analyzed through relationship software programs or key word search programs, this should also be planned out at this time. These tasks should be integrated into a written investigation or work plan so that the entire process going forward is documented. Also, if there is a variation from the written investigation plan, such variation should be documented and an explanation provided as to why there was such a variation. Lastly, if international travel is involved, this should also be considered and planned for at this step. Step 2 should be accomplished within another one to three days.

Step 3: Executing the investigation plan

Under this step, the investigation should be completed. I would urge that the interviews not be undertaken until all documents are reviewed and ready for use. Care should be taken to ensure that an appropriate "*Upjohn* warning" is issued and that the interviewee clearly understands that whoever is performing the interview represents the company, and not the person being interviewed, whether they are the target of the investigation or not. The appropriate steps should also be taken to preserve the attorney-client privilege and attorney work

product assertions. Step 3 should be accomplished in one to two weeks.

Step 4: Determining appropriate follow-up

At this step, the preliminary investigation should be completed and you will be ready to move into the final phases. In some investigations, it is relatively easy to determine when the work is essentially complete. For example, if the allegation is both specific and narrow, and the investigation reveals a compelling and benign explanation for the conduct alleged, then the investigation typically is complete and you are ready to convene the investigation team and the relevant business unit representatives. This group would decide on the appropriate disciplinary steps or other actions to take. Step 4 should be completed in one day to one week.

It must be cautioned that, at this step, if there are findings of specific or discrete allegations of corruption and bribery, a decision must be made as to how to handle such findings going forward.

Step 5: Closing the case

Under this final step, you should communicate the investigation results to the stakeholders and complete the case report. Everything done in the above steps should be documented and stored together, either electronically or in hard copy form. The case report should be completed. Step 5 should be completed in one day to one week.

Use of specialized counsel in a FCPA investigation

In an *ACC Docket* article, James McGrath and David Hildebrandt write that when faced with an issue such as an alleged FCPA violation, a company should engage "specialized" counsel to perform the investigation.[9] There were three reasons for this suggestion to use specialized counsel. The first is that the DOJ would look toward the independence and impartiality of such investigations as one of its factors in favor of declining or deferring enforcement. If in-house counsel headed up the investigation, the DOJ might well deem the investigative results "less than trustworthy".

A second reason came from the company perspective. Many companies have sought protection of investigations behind the shield of the attorney-client privilege and attorney work-product doctrine. If an in-house attorney is utilized, many courts are skeptical of a company asserting these privileges because of the mixed responsibilities of counsel in a corporation: those relating to legal

and business work. As noted by Russ Berland in his article in *Compliance & Ethics Professional*, some courts "presume that in-house counsel engage in a substantial amount of non-legal work".[10] Additionally, obstructionist attempts by corporations to improperly assert attorney-client privilege have led courts to refuse to allow the privilege to be asserted altogether. However, a company will usually not face these arguments if outside counsel is utilized.

Even if the company is willing to waive its attorney-client privilege, McGrath and Hildebrandt offer a third reason for the use of specialized outside counsel to handle an investigation. If a company's regular outside counsel were retained to conduct the investigation, the DOJ might feel the results had less than full credibility because the law firm knew "who buttered its bread"; the firm would not want to bring bad news to client and endanger an ongoing business relationship. The authors conclude by pointing out that employing specialized counsel comports with the expectations under the US Sentencing Guidelines, gives a company the protections of attorney-client privilege and the work-product doctrine, and, finally, "assures the government of the integrity of the internal investigation".

I would add a couple more reasons to those listed by Hildebrandt and McGrath. If there are serious allegations made concerning your company's employees engaging in criminal conduct, a serious response is required. Your company needs to hire some seriously good lawyers to handle any internal investigation. These lawyers need to have independence from the company so do not call your regular corporate counsel. Hire some seriously good investigative lawyers.

I believe that there is another reason to hire outside counsel. It is also important because, no matter what the outcome of your investigation, you will most probably have to deal with the government. If the investigation does reveal actionable conduct, your company will need legal counsel who is most probably an ex-DOJ prosecutor or ex-AUSA to get your company through that process. Even if there is a finding of no criminal activity, you will need very competent and very credible counsel to explain the investigation protocol and its results to the government.

References

1. Volkov, M., "Encouraging Communication of Employee Concerns", *Corruption, Crime & Compliance*, 27 March 2014, see corruptioncrimecompliance.com/2014/03/encouraging-communication-of-employee-concerns.

2. Tabuena, J., "Promoting Effective Use of the Compliance hotline", *Compliance Week*, 1 August 2012.
3. Wearden, G., "GlaxoSmithKline whistleblower awarded $96m payout", the *Guardian*, 27 October 2010, see www.theguardian.com/business/2010/oct/27/glaxosmithkline-whistleblower-awarded-96m-payout.
4. Matthews, C.M., and Rubenfeld, S., "NCR Investigates Alleged FCPA Violations", *Wall Street Journal* Blogs, 13 August 2012, see blogs.wsj.com/corruption-currents/2012/08/13/ncr-investigates-alleged-fcpa-violations.
5. Matthews, C.M., "NCR Discloses SEC Subpoena Related to Whistleblower", *Wall Street Journal* Blogs, 18 October 2012, see blogs.wsj.com/corruption-currents/2012/10/18/ncr-dislcoses-sec-subpoena-related-to-whistlblower.
6. Hoyos, C., "Emails tell of fears over EADS payments", *Financial Times*, 14 August 2012, see www.ft.com/cms/s/0/0d99a2ae-e562-11e1-9a2f-00144feab49a.html.
7. Ethics Resource Center (ERC), white paper, "Blowing the Whistle on Workplace Misconduct", December 2010, see www.ethics.org/files/u5/WhistleblowerWP.pdf.
8. Volkov, M., "How to Prevent Whistleblower Complaints", *Corruption, Crime & Compliance*, 29 January 2013, see corruptioncrimecompliance.com/2013/01/how-to-prevent-whistleblower-complaints.
9. McGrath, J., and Hildebrandt, D., "Risks and Rewards of Independent Internal Investigations", *ACC Docket*, October 2010.
10. Berland, R., "How to Protect Compliance Risk Assessments from an Unwanted Disclosure", *Compliance & Ethics Professional*, vol. 7, no. 5, October 2010.

Chapter 9: How to get better

YOU SHOULD keep track of external and internal events which may cause changes to business process, policies, and procedures. Some examples are new laws applicable to your business organization and internal events which drive changes within a company. Such internal changes could be a company reorganization or major acquisition. This type of review appears to be similar to the DOJ advocacy of ongoing risk assessments. The FCPA Guidance specifies that "a good compliance program should constantly evolve. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the standards of its industry. In addition, compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements. Consequently, DOJ and SEC evaluate whether companies regularly review and improve their compliance programs and not allow them to become stale."

Continuous improvement requires that you not only audit but also monitor whether employees are continuing to follow the compliance program. In addition to the language set out in the FCPA Guidance, 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 activities are key components enforcement officials look for when determining whether companies maintain adequate oversight of their compliance programs.

A review plan is an excellent tool for the compliance practitioner because it provides a method for the ongoing evaluation of policies and sets forth a manner to communicate and train on any changes which are implemented. More than simply staying current, this approach will help provide the dynamics that the DOJ continually stresses are essential to keeping your program

fresh. Lastly, such a review plan can also guide the compliance practitioner in creating an ongoing game plan for compliance program upgrades and updates.

The FCPA Guidance makes clear that each company should assess its risks and manage its risks. The Guidance specifically notes that small and medium-size enterprises likely will have different risk profiles and therefore different attendant compliance programs than large multi-national corporations. Moreover, this is something that the DOJ and SEC take into account when evaluating a company's compliance program in any FCPA investigation. This is why a "check-the-box" approach is disfavored by the DOJ, and, at the end of the day, it is also ineffectual. This is because each compliance program should be tailored to the enterprise's own specific needs, risks, and challenges.

One tool that is extremely useful in the continuous improvement cycle is ongoing monitoring, yet is often misused or misunderstood. This may come from the confusion surrounding the differences between "monitoring" and "auditing". "Monitoring" is a commitment to reviewing and detecting compliance variances 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 across a wide spectrum of data and information.

"Auditing", on the other hand, 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. You should not assume that because your company conducts audits that it is effectively "monitoring"; a robust program should include separate functions for auditing and monitoring. Although 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 in order 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 have noticed recent accounting irregularities. Regional directors should be required to keep tabs

on potential improper activity in the countries in which they manage. These ongoing efforts demonstrate that your company is serious about compliance.

The DOJ emphasized again, with the 2011 Pfizer DPA, the need for a company to establish protocols for auditing. It included the following detail on auditing protocols:

- 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;
- Review of a representative sample (appropriately adjusted for the risks of the market) of contracts with and payments to individual foreign government officials as well as other high-risk transactions in the market;
- Creation of action plans resulting from issues identified during the proactive reviews, which 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
- A review of the books and records of a sample of third-party representatives which, in the view of the FCPA proactive review team, may present a corruption risk. Prior to such an investigation, however, the company should have procedures in place to make sure every investigation is thorough and authentic, including document preservation protocols, data privacy policies, and communication systems designed to manage and deliver information efficiently.

Six steps to implementing continuous monitoring in your compliance program

Anti-corruption, anti-bribery, and anti-money laundering programs, policies, and procedures, and even export control systems, are seemingly in a constant state of evolution. Many companies are struggling with the challenge of implementing effective controls and monitoring risks across a spectrum that could include the three above-listed compliance areas as well as others. One area which has evolved into a minimum best practices requirement for compliance is that of continuous monitoring.

While many companies will look at continuous monitoring as a software solution that can assist your company in managing risk, provide reporting metrics, and thereby insights across an organization, it should be viewed more

holistically. You will need to take in many disparate systems, usually across a wide international geographic area, which may seem like an overwhelming process. Justin Offen, explained this in his article, "Mission Impossible? Six steps to continuous monitoring".[1] He detailed a six-point program to ensure that your "CM solution doesn't become part of the problem", rather than a solution:

1. Know your global IT footprint: It is important to understand how continuous monitoring will be incorporated into your company's overall IT strategy as well as your compliance strategy. This inquiry should begin with understanding what your current IT structure is and what it is anticipated to be in three and five years. Once you identify your global IT footprint, you can determine which system will be the best fit.
2. Define scope and necessary resources: You should determine what your goal is; begin by identifying your needs, and then prioritize them. You should perform a risk analysis and then rank the risks. Next, you need to understand the amount of talent you have in your organization, identify who can implement and work with the system, and determine your budget, which may need to be increased based upon your need for outside experts and unknown contingencies.
3. Conduct a pilot or proof of concept: A phased roll-out can be used as a "proof of concept", which can yield greater functioning efficiency throughout your entire program implementation. It should also allow you to chalk up an early success to present to the inevitable nay-sayers in your organization.
4. Decrease false positives: This is important because improper or incomplete testing may well lead to a larger amount of false positives, which you are required to evaluate and clear. From each test, you can further refine your continuous monitoring solution to the specific needs of your organization and increase time and efficiency in your overall continuous monitoring program.
5. Establish your escalation protocol: You should establish a response protocol when an exception or red flag arises. This protocol should include an escalation protocol, if the red flag suggests that it is warranted, or additional investigation determines a wider problem exists. This protocol should include specific individuals and departments that need to be notified, the makeup of your initial and secondary triage team, and the accountability for each person in the process, all the way up to the board.

6. Demonstrate control through case management: This demonstrates once again the maxim of document, document, and document. You need to be ready to "respond with appropriate documentation of any transaction that's been reviewed, showing the level of review and any additional steps taken".

The benefits of such a continuous monitoring program are significant: the creation of documentation which can lead to a "ready response" by a company to an issue before it becomes a larger problem, coupled with the ability to recall all steps and information when a regulator comes knocking. Internally, using the pilots or proofs of concepts, the compliance department can bring in other stakeholders to see the value of continuous monitoring within the organization.

You have a strategic plan; now what do you do?

Have you thought about your anti-corruption policy through the lens of a strategic plan? If not, you might want to use the formulation proffered by Bruce Rector, in an article entitled "Strategic planning needs constant follow-up to be successful".[2] Recognizing that a strategic plan can serve as guide for your company going forward, it must actually be *implemented* to garner any use out of it. I believe that the steps he lays out translate without difficulty into steps a compliance officer can take to meet the suggestions laid out by Offen above:

- Review the goals of the strategic plan: This requires that you arrange a time for the CCO and team to review the goals of the strategic plan. To the extent possible, this should be done in person. The CCO should lead a discussion of the strategic plan and determine how a certain goal in the plan measures up to its implementation in your company.
- Design an execution plan: The "keep it simple, sir" or KISS method is the best to move forward. This would suggest that, for each compliance goal, there should be a simple and straightforward plan to ensure that the goal in question is being addressed. Any such plan must be specific and clear for all involved with tasks handed out, deliverables, and a definite timeline for delivery.
- Put accountabilities in place: In any plan of execution, there must be accountabilities attached. Simply having a timeline is not enough. This means that those persons with the responsibility for performing tasks be clearly identified, along with the specific task they are assigned to

complete. Accountability requires that there be follow-up to confirm that these targets are met. This requires the CCO or other senior compliance department representative to put these in place and then mandate a report requirement on how the task assigned is being achieved.

- Schedule the next review of the plan: There should be a regular review of the process. While noting that this may seem time consuming, this can be a group responsibility, which will assist the process moving forward more smoothly. It also allows any problems which may arise to be detected and corrected more quickly than if meetings are held on a less frequent basis.

It is a role of the CCO to reinforce the vision and goals of the compliance function, where assessment and updating are critical to an ongoing best practices compliance program. If you follow this protocol, you will put a mechanism in place to demonstrate your company's commitment to compliance by following through on intentions as set forth in your strategic plan.

The regulator's perspective

What does an effective compliance program look like? Over the years, we have heard various formulations of inquiries that regulators might use when reviewing a compliance program. As is obvious from the number of times I have referenced "McNulty's maxims" in this report, one of my favorite approaches is to use the three questions that former US deputy attorney general and Baker & McKenzie LLP partner Paul McNulty identified as three general areas of inquiry he would assess regarding an enforcement action when he was at the DOJ. To reiterate, they are:

- Maxim No. 1: "What did you do to stay out of trouble?"
- Maxim No. 2: "What did you do when you found out?" and
- Maxim No. 3: "What remedial action did you take?"

Andrew Ceresney, director of the Division of Enforcement at the SEC, speaking at Compliance Week 2014, said that he has "found that you can predict a lot about the likelihood of an enforcement action by asking a few simple questions about the role of the company's legal and compliance departments in the firm". He then went on to detail some rather straightforward questions that he believes can show just how much a company is committed to having a robust compliance regime:

- Are legal and compliance personnel included in critical meetings?
- Are their views typically sought and followed?
- Do legal and compliance officers report to the CEO and have significant visibility with the board?
- Are the legal and compliance departments viewed as an important partner in the business and not simply as support functions or a cost center?

Near the end of his presentation, Cerensey said that "Far too often, the answer to these questions is 'no', and the absence of real legal and compliance involvement in company deliberations can lead to compliance lapses, which, in turn, result in enforcement issues. When I was in private practice, I always could detect a significant difference between companies that prioritized legal and compliance and those that did not. When legal and compliance were not equal partners in the business, and were not consulted as a matter of course, problems were inevitable."

Along with McNulty's maxims, Cerensey's questions provide significant guideposts to how regulators think about FCPA compliance programs. For me, I think the point is that companies that actually "do compliance" are easy to spot. For all the gnashing of teeth about how hard it is to comply with what the DOJ and SEC want to see in FCPA compliance, when the true focus can be distilled into whether a company actually "does" compliance, as opposed to saying how ethical they are, I think it simplifies the inquiry and the issues senior management and a board of directors really need to pay attention to.

Continuous improvement through continuous monitoring or other techniques will help keep your compliance program abreast of any changes in your business model's compliance risks, and allow growth based upon new and updated best practices specified by regulators. A compliance program is in many ways a continuously evolving organism, just as your company is. You need to build in a way to keep pace with both market and regulatory changes to have a truly effective anti-corruption compliance program. The FCPA Guidance makes clear that the "DOJ and SEC will give meaningful credit to thoughtful efforts to create a sustainable compliance program if a problem is later discovered. Similarly, undertaking proactive evaluations before a problem strikes can lower the applicable penalty range under the US Sentencing Guidelines. Although the nature and the frequency of proactive evaluations may vary depending on the size and complexity of an organization, the idea behind such efforts is the same: continuous improvement and sustainability."

References

1. Offen, J., "Mission Impossible? Six steps to continuous monitoring", *Compliance Week*, November 2011.
2. Rector, B., "Strategic planning needs constant follow-up", *Houston Business Journal*, 11 November 2011, see www.bizjournals.com/houston/print-edition/2011/11/11/strategic-planning-needs-constant.html?page=all.

Chapter 10: Should I or shouldn't I? Mergers and acquisitions

THE FCPA Guidance makes clear that one of the ten hallmarks of an effective compliance program centers on mergers and acquisitions (M&A) in both the pre- and post-acquisition context. A company that does not perform adequate FCPA due diligence prior to a merger or acquisition may face both legal and business risks. Perhaps most commonly, inadequate due diligence can allow a course of bribery to continue – with all the attendant harms to a business's profitability and reputation, as well as potential civil and criminal liability. By contrast, companies that conduct effective FCPA due diligence on their acquisition targets are able to evaluate more accurately each target's value and negotiate for the costs of the bribery to be borne by the target.

Equally important, however, is that if a company engages in the suggested actions, they will go a long way towards insulating, or at least lessening, the risk of FCPA liability going forward. Nathaniel Edmonds, in an interview in the *Wall Street Journal*, said "I think most companies and their outside counsel believe any potential corruption problem should stop a deal from occurring. Companies would be surprised to learn that neither the Securities and Exchanges Commission nor the DOJ takes that position. In many ways the SEC and DOJ encourage good companies with strong compliance programs to buy the companies engaged in improper conduct in order to help implement strong compliance in companies that have engaged in wrongful conduct. What companies must do and what outside counsel should advise them to do is to have a realistic perspective of what effect that corruption or potential improper payment has on the value of the deal itself. Because of the concern that any corruption would stop the deal or implicate the buyers, many times companies don't look as thoroughly as they should at potential corruption. There is often concern that if you start to

look for something you may find a problem and it could slow down or stop the whole deal."[1]

The FCPA Guidance was the first time that many compliance practitioners focused on the pre-acquisition phase of a transaction as part of a compliance regime. However, the DOJ and the SEC made clear the importance of this step. In addition to the above language, they cited another example in the section on declinations where the "DOJ and SEC declined to take enforcement action against a US publicly held consumer products company in connection with its acquisition of a foreign company."

The steps taken by the company led the Guidance to state the following: "The company identified the potential improper payments to local government officials as part of its pre-acquisition due diligence and the company promptly developed a comprehensive plan to investigate, correct, and remediate any FCPA issues after acquisition".

In a hypothetical, the FCPA Guidance provided some specific steps a company had taken in the pre-acquisition phase. These steps included, "(1) having its legal, accounting, and compliance departments review Foreign Company's sales and financial data, its customer contracts, and its third-party and distributor agreements; (2) performing a risk-based analysis of Foreign Company's customer base; (3) performing an audit of selected transactions engaged in by Foreign Company; and (4) engaging in discussions with Foreign Company's general counsel, vice president of sales, and head of internal audit regarding all corruption risks, compliance efforts, and any other corruption-related issues that have surfaced at Foreign Company over the past ten years."

Pre-acquisition risk assessment

It should all begin with a preliminary pre-acquisition assessment of risk. Such an early assessment will inform the transaction research and evaluation phases. This could include an objective view of the risks faced and the level of risk exposure, such as best/worst case scenarios. A pre-acquisition risk assessment could also be used as a "lens through which to view the feasibility of the business strategy" and help to value the potential target.

The next step is to develop the risk assessment as a base document. From this document, you should be able to prepare a focused series of queries and requests to be obtained from the target company. Thereafter, company management can use this pre-acquisition risk assessment to attain what might be required in the way of integration post-acquisition. It would also help to

inform how the corporate and business functions may be affected. It should also assist in planning for timing and anticipation of the overall expenses involved in post-acquisition integration. These costs are not insignificant and they should be thoroughly evaluated in the decision-making calculus.

A five-step process for pre-acquisition due diligence

Next is a five-step process on how to plan and execute a strategy to perform pre-acquisition due diligence in the M&A context:

1. Establish a point of contact: Here you need to determine one point of contact that you can liaise with throughout the process. Typically, this would be the target's CCO if the company is large enough to have this full-time position.
2. Collect relevant documents: Obtain a detailed list of sales going back three to five years, broken down by country, and, if possible, obtain a further breakdown by product and/or services; all joint venture (JV) contracts, due diligence on JVs, and other third party business partners; the travel and entertainment records of the acquisition target company's top sales personnel in high-risk countries; internal audit reports; and other relevant documents. You do not need to investigate de minimis sales amounts but focus your compliance due diligence inquiry on high sales volumes in high-risk countries. If the acquisition target company uses a sales model of third parties, obtain a complete list, including JVs. It should be broken out by country and amount of commission paid. Review all underlying due diligence on these foreign business representatives, their contracts, and how they were managed after the contract was executed, your focus should be on large commissions in high-risk countries.
3. Review the compliance and ethics mission and goals: Here you need to review the code of conduct or other foundational documents that a company might have to gain some insight into what they publicly espouse.
4. Review the seven elements of an effective compliance program as listed below:
    i. Oversight and operational structure of the compliance program: Here you should assess the role of board, CCO, and, if there is one, the compliance committee. Regarding the CCO, you need to look at their reporting and access – is it independent within the overall structure of the company? Also, what are the resources dedicated to the

compliance program, including a review of personnel, the budget, and overall resources? Review high-risk geographic areas where your company and the acquisition target company do business. If there is overlap, seek out your own sales and operational people and ask them what compliance issues are prevalent in those geographic areas. If there are compliance issues that your company faces, then the target probably faces them as well.

ii. Policies/procedures, code of conduct: In this analysis you should identify industry practices and legal standards that may exist for the target company. You need to review how the compliance policies and procedures were developed and determine the review cycles, if any. Lastly, you need to know how everything is distributed and what the enforcement mechanisms for compliance policies are. Additionally, you need to validate with HR if there have been terminations or disciplines relating to compliance.

iii. Education, training, and communication: Here you need to review the compliance training process as it exists in the company, both the formal and the informal. You should ask questions, such as "What are the plans and schedules for compliance training?" Next, determine if the training material itself is fit for its intended purpose, including both internal and external training for third parties. You should also evaluate the training delivery channels, for example is the compliance training delivered live, online, or through video? Finally, assess whether the company has updated their training based on changing of laws. You will need to interview the acquisition target company personnel responsible for its compliance program to garner a full understanding of how they view their program. Some of the discussions that you may wish to engage in include visiting with the target company's general counsel (GC), its vice president of sales and head of internal audit regarding all corruption risks. You should also delve into the target's compliance efforts, and any other corruption-related issues that may have surfaced.

iv. Monitoring and auditing: Under this section you need to review both the internal audit plan and methodology used regarding any compliance audits. A couple of key points are (1) is it consistent over a period of time and (2) what is the audit frequency? You should also try to judge whether the audit is truly independent or if there

was manipulation by the business unit(s). You will need to review the travel and entertainment records of the acquisition target company's top sales personnel in high-risk countries. You should retain a forensic auditing firm to assist you with this effort. Use the resources of your own company personnel to find out what is reasonable for travel and entertainment in the same high-risk countries in which your company does business.

v. Reporting: What is the company's system for reporting violations or allegations of violations? Is the reporting system anonymous? From there, you need to turn to who does the investigations to determine how they are conducted. A key here, as well as something to keep in mind throughout the process, is the adequacy of record keeping by the target.

vi. Response to detected violations: This review is to determine management's response to detected violations. What corrective action has been taken to prevent future, similar violations? Has there been any internal enforcement and discipline of compliance policies if there were violations? Lastly, what are the disclosure procedures to let the relevant regulatory or other authorities know about any violations and the responses thereto? Further, you may be required to self-disclose any FCPA violations that you discover. There may be other reporting issues in the M&A context, such as any statutory obligations to disclose violations of any anti-bribery or anti-corruption laws in the jurisdiction(s) in question; what effect will disclosure have on the target's value or the purchase price that your company is willing to offer?

vii. Enforcement practices/disciplinary actions: Under this analysis, you need to see if there was any discipline delivered up to and including termination. If remedial measures were put in place, how were they distributed throughout the company and were they understood by employees?

5. Periodically, evaluate the M&A review procedures' effectiveness benchmarked against any legal proceedings, FCPA enforcement actions, opinion procedure releases, or other relevant information.

Finally, while you are performing the anti-corruption due diligence, you should also review issues for anti-money laundering (AML) and export control issues.

What should you do with the information that you uncover in your pre-acquisition due diligence?

Jay Martin, CCO at BakerHughes Inc. suggests an approach based on the review of key risk factors. Martin has laid out 15 key risk factors, which he believes should prompt a purchaser to conduct heightened due diligence, or even to reconsider moving forward with an acquisition under extreme circumstances:

1. A presence in a BRIC (Brazil, Russia, India and China) country and other countries where corruption risk is high, for example, a country with a Transparency International CPI rating of 5 or less;
2. Participation in an industry that has been the subject of recent anti-bribery or FCPA investigations, for example, in the oil and energy, telecommunications, or pharmaceuticals sectors;
3. Significant use of third-party agents, for example, sales representatives, consultants, distributors, subcontractors, or logistics personnel (customs, visas, freight forwarders, etc.);
4. Significant contracts with a foreign government or instrumentality, including state-owned or state-controlled entities;
5. Substantial revenue from a foreign government or instrumentality, including a state-owned or state-controlled entity;
6. Substantial projected revenue growth in the foreign country;
7. High amount or frequency of claimed discounts, rebates, or refunds in the foreign country;
8. A substantial system of regulatory approval, for example, for licenses and permits, in the country;
9. A history of prior government anti-bribery or FCPA investigations or prosecutions;
10. Poor or no anti-bribery or FCPA training;
11. A weak corporate compliance program and culture, in particular from legal, sales, and finance perspectives at the parent level or in foreign country operations;
12. Significant issues in past FCPA audits, for example, excessive undocumented entertainment of government officials;
13. The degree of competition in the foreign country;
14. Weak internal controls at the parent or in foreign country operations; and
15. In-country managers who appear indifferent or uncommitted to US laws, the FCPA, and/or anti-bribery laws.

It is also important that after the due diligence is completed, and if the transaction moves forward, the acquiring company should attempt to protect itself through the most robust contract provisions that it can obtain; these would include indemnification against possible FCPA violations, including both payment of all investigative costs and any assessed penalties. An acquiring company should also include representations (reps) and warranties in the final sales agreement that the entire target company uses for participation in transactions as permitted under local law: that there is an absence of government owners in company; that the target company has made no corrupt payments to foreign officials; and that all the books and records presented to the acquiring company for review were complete and accurate.

To emphasize all of the above, the DOJ stated in the Pfizer deferred prosecution agreement (DPA) that, in the M&A context, a company is to ensure that, when practicable and appropriate, new business entities are only acquired after thorough risk-based FCPA and anti-corruption due diligence is conducted by a suitable combination of legal, accounting, and compliance personnel. When such anti-corruption due diligence is appropriate but not practicable prior to acquisition of a new business for reasons beyond a company's control, or due to any applicable law, rule, or regulation, an acquiring company should continue to conduct anti-corruption due diligence subsequent to the acquisition and report to the DOJ of any corrupt payments or falsified books and records.

1. Post-acquisition integration

Previously, many compliance practitioners had based decisions in the M&A context on DOJ Opinion Procedure Release 08-02, which related to Halliburton's proposed acquisition of the UK entity, Expro.[2] In the spring of 2011, the Johnson & Johnson (J&J) DPA changed the perception of compliance practitioners regarding what is required of a company in the M&A setting related to FCPA due diligence, both pre- and post-acquisition. On 18 June 2012, the DOJ released the Data Systems & Solutions LLC (DS&S) DPA which brought additional information to the compliance practitioner on what a company can do to protect itself in the context of M&A activity.

08-02 began as a request from Halliburton to the DOJ from issues that arose in the pre-acquisition due diligence of the target company, Expro. Halliburton had submitted a request to the DOJ specifically posing these three questions:

1. Whether the proposed acquisition transaction itself would violate the FCPA;
2. Whether, through the proposed acquisition of target, Halliburton would "inherit" any FCPA liabilities of target for pre-acquisition unlawful conduct; and
3. Whether Halliburton would be held criminally liable for any post-acquisition unlawful conduct by target prior to Halliburton's completion of its FCPA and anti-corruption due diligence, where such conduct is identified and disclosed to the department within 180 days of closing.

Halliburton

Halliburton committed to the following conditions in 08-02, if it was the successful bidder in the acquisition:

1. Within ten business days of the closing, Halliburton would present to the DOJ a comprehensive, risk-based FCPA and anti-corruption due diligence work plan which would address, among other things, the use of agents and other third parties; commercial dealings with state-owned customers; any joint venture, teaming, or consortium arrangements; customs and immigration matters; tax matters; and any government licenses and permits. The Halliburton work plan committed to organizing the due diligence effort into "high risk", "medium risk", and "lowest risk" elements.
   i. Within 90 days of closing: Halliburton would report to the DOJ the results of its high risk due diligence;
   ii. Within 120 days of closing: Halliburton would report to the DOJ the results to date of its medium risk due diligence;
   iii. Within 180 days of closing: Halliburton would report to the DOJ the results to date of its lowest risk due diligence; and
   iv. Within one year of closing: Halliburton committed full remediation of any issues which it discovered thus far.

This opinion procedure release laid out a clear road map for dealing with some of the difficulties inherent in conducting sufficient pre-acquisition due diligence in the FCPA context. Indeed, the DOJ concluded 08-02 by noting, "Assuming that Halliburton, in the judgment of the Department, satisfactorily implements the post-closing plan and remediation detailed above… the Department does not presently intend to take any enforcement action against Halliburton."

Johnson & Johnson

In Attachment D of the J&J DPA, entitled "Enhanced Compliance Obligations", there is a list of compliance obligations in which J&J agreed to undertake certain enhanced compliance obligations for at least the duration of its DPA, beyond the minimum best practices also set out in the J&J DPA. With regard to the M&A context, J&J agreed to the following:

1. J&J will ensure that new business entities are only acquired after thorough FCPA and anti-corruption due diligence by legal, accounting, and compliance personnel. Where such anti-corruption due diligence is not practicable prior to acquisition of a new business for reasons beyond J&J's control, or due to any applicable law, rule, or regulation, J&J will conduct FCPA and anti-corruption due diligence subsequent to the acquisition and report to the department any corrupt payments, falsified books and records, or inadequate internal controls as required by the deferred prosecution agreement.
2. J&J will ensure that J&J's policies and procedures regarding the anti-corruption laws and regulations apply as quickly as is practicable, but in any event no less than one year post-closing, to newly-acquired businesses, and will promptly, for those operating companies that are determined not to pose corruption risk, J&J will conduct periodic FCPA audits, or will incorporate FCPA components into financial audits.
3. J&J will train directors, officers, employees, agents, consultants, representatives, distributors, joint venture partners, and relevant employees thereof, who present corruption risk to J&J, on the anti-corruption laws and regulations and J&J's related policies and procedures.
4. J&J will conduct an FCPA-specific audit of all newly acquired businesses within 18 months of acquisition.

Data Systems & Solutions LLC (DS&S)

In the DS&S DPA, there were two new items listed in the corporate compliance program, relating to M&A, which read:

1. DS&S will develop and implement policies and procedures for mergers and acquisitions requiring that DS&S conduct appropriate risk-based due diligence on potential new business entities, including appropriate FCPA and anti-corruption due diligence by legal, accounting, and compliance

personnel. If DS&S discovers any corrupt payments or inadequate internal controls as part of its due diligence of newly acquired entities or entities merged with DS&S, it shall report such conduct to the Department as required in Appendix B of this Agreement.

2. DS&S will ensure that DS&S's policies and procedures regarding the anti-corruption laws apply as quickly as is practicable to newly acquired businesses or entities merged with DS&S and will promptly:
   i. Train directors, officers, employees, agents, consultants, representatives, distributors, joint venture partners, and relevant employees thereof, who present corruption risk to DS&S, on the anti-corruption laws and DS&S's policies and procedures regarding anti-corruption laws.
   ii. Conduct an FCPA-specific audit of all newly acquired or merged businesses as quickly as practicable.

This language draws from and builds upon the prior opinion release, 08-02, regarding Halliburton's request for guidance and the J&J "enhanced compliance obligations" incorporated into its DPA. While the DS&S DPA does note that it is specifically tailored as a solution to DS&S's FCPA compliance issues, I believe that this is the type of guidance that a compliance practitioner can rely upon when advising clients on what the DOJ expects during M&A activities.

The FCPA Guidance, coupled with 08-02 and the two enforcement actions, speak to the importance that the DOJ puts on M&A in the FCPA context. The time frames for post-acquisition integration are quite tight. This means that you should do as much work as you can in the pre-acquisition stage. The DOJ makes clear that rigor is needed throughout your entire compliance program, including M&A. This rigor should be viewed as something more than just complying with the FCPA; it should be viewed as simply good business sense.

Time frames	Halliburton 08-02	J&J	DS&S
FCPA audit	High-risk agents – 90 days Medium-risk agents – 120 Days Low-risk Agents – 180 days	18 months to conduct full FCPA audit	As soon "as practicable"
Implement FCPA compliance program	Immediately upon closing	12 months	As soon "as practicable"
Training on FCPA compliance program	60 days to complete training for high-risk employees, 90 days for all others	12 months to complete training	As soon "as practicable"

Table 1: FCPA M&A box score summary

In his interview with the *Wall Street Journal*, former DOJ attorney Nathaniel Edmonds emphasized that if a company does not have the opportunity to make these types of inquiries in the pre-acquisition stage, "if there are good faith efforts to conduct due diligence, integrate compliance programs and take remedial actions by removing those wrongdoers — if all of that is done on a quick basis [authorities] give very strong credit. The best example of this is the 2009 purchase by Pfizer of Wyeth. I was prosecutor on the Pfizer Wyeth [bribery] case. Pfizer was able to do some due diligence before the acquisition but because both are massive organizations it was not possible to do complete due diligence prior to acquisition. But after the acquisition within 180 days they had identified much of the wrongdoing at Wyeth and ensured it was halted. As a result of that we gave them credit. On the criminal side Pfizer was not held criminally liable for any of the conduct at Wyeth. Most of what Pfizer was held responsible for was as a result of a previous acquisition of Pharmacia, which they acquired in 2002 and 2003. At the time of the Pharmacia acquisition, acquirers did not typically conduct anti-corruption due diligence on

targets. And during the investigation most of the violations of FCPA [Pfizer] was held criminally liable for began prior to the acquisition of Pharmacia – some was afterwards. Pfizer was held responsible for the misconduct at Pharmacia both before and afterwards. The Pfizer case is interesting because it shows both the good and bad."

References

1. Schectman, J., "Former Justice Official: How to Buy Corrupt Companies", *Wall Street Journal* Blogs, 26 June 2014, see blogs.wsj.com/riskandcompliance/2014/06/26/former-justice-official-on-how-to-buy-corrupt-companies.
2. FCPA Opinion Procedure Release, No. 08-02, 13 June 2008.

Chapter 11: A few words about facilitation payments

ONE OF the more confusing areas of the FCPA is in that of facilitation payments. Facilitation payments are small bribes, but make no mistake about it, they *are* bribes. For that reason, many companies feel they are inconsistent with a company culture of doing business ethically and in compliance with laws prohibiting corruption and bribery. Further, the FCPA Guidance specifies that "while the payment may qualify as an exception to the FCPA's anti-bribery provisions, it may violate other laws, both in Foreign Country and elsewhere. In addition, if the payment is not accurately recorded, it could violate the FCPA's books and records provision."

Interestingly, in recent remarks, Thomas C. Baxter, executive vice president and general counsel at the Federal Reserve Bank of New York indicated a general unease with facilitation payments. Baxter's comments on the subject were referenced in the *FCPA Blog* as follows:[1] "Baxter said an organizational policy that allows some types of official corruption – including facilitating payments – 'diminishes the efficacy of compliance rules that are directed toward stopping official corruption.'" As reported, he said, "While I understand that the exception is grounded in a practical reality, I feel that zero tolerance for official corruption would have been a better choice. To any public servant with an extended hand, I would say in a loud and clear voice, "pull it back and do your job. And, let me note the OECD Working Group on Bribery recommends that all countries encourage companies to prohibit or discourage facilitating payments."

In addition to these clear statements about whether the FCPA should continue allow "small" bribes, you should also consider the administrative nightmare these pose for any international company. The UK Bribery Act does not have any such exception, exemption, or defense along the lines of the

FCPA facilitation payment exception. This means that even if your company allows facilitation payments, it must exempt every UK company or subsidiary from the policy. Further, if your company employs any UK citizens, they are subject to the UK Bribery Act no matter whom they work for and where they work in the world, so they must also be exempted. Finally, if your US company does business with a UK or other company subject to the UK Bribery Act, you may be prevented contractually from making facilitation payments while working under that customer's contract.

The statute

When the FCPA was initially passed in 1977, the facilitating payment exception was found under the definition of "foreign official". However, with the 1988 Amendments, a more explicit exception was written into the statute, making it clear that the anti-bribery provisions "shall not apply to any facilitating or expediting payment to a foreign official, political party, or party official the purpose of which is to expedite or to secure the performance of a routine governmental action…"

The statute itself provided a list of examples of facilitation payments in the definition of routine governmental actions. It included the following:

- Obtaining permits, licenses, or other official documents;
- Processing governmental papers such as visas and work orders;
- Providing police protection, mail services, scheduling inspections; and
- Providing utilities, cargo handling, or actions of a similar nature.

It is important to note that the language of the FCPA makes it clear that a facilitation payment is not an affirmative defense but an exception to the general FCPA proscription against bribery and corruption. Unfortunately for the FCPA practitioner, there is no dollar limit articulated in the FCPA regarding facilitation payments. Even this limited exception has come under increasing criticism. As far back as 2009, the OECD studied the issue and recommended that member countries encourage their corporations not to allow the making of facilitating payments, "in view of the corrosive effect of small facilitation payments, particularly on sustainable economic development and the rule of law".

Enforcement actions and a declination

Con-way

The FCPA landscape is littered with companies who sustained FCPA violations due to payments which did not fall into the facilitation payment exception. In 2008, Con-way, a global freight forwarder, paid a $300,000 penalty for making hundreds of relatively small payments to customs officials in the Philippines. The value of the payments Con-way was fined for making totaled $244,000 and were made to induce the officials to violate customs regulations, settle customs disputes, and reduce or not otherwise enforce legitimate fines for administrative violations.

Helmerich and Payne

In 2009, Helmerich and Payne paid a penalty and disgorgement fee of $1.3 million for payments which were made to secure customs clearances in Argentina and Venezuela. The payments ranged from $2,000 to $5,000, but were not properly recorded, and were made to import/export goods that were not within the respective country's regulations, to import goods that could not lawfully be imported, and to evade higher duties and taxes on the goods.

Panalpina

Then there is the Panalpina enforcement action. This matter was partly resolved last year with the payment by Panalpina and six of its customers of over $257 million in fines and penalties. Panalpina, acting as freight forwarder for its customers, made payments to circumvent import laws, reduce customs duties and tax assessments, and to obtain preferential treatment for importing certain equipment into various countries, but primarily into West Africa.

DynCorp

Finally, the DynCorp investigation matter related to some $300,000 in payments made by subcontractors who wished to speed up their visa processing and expedite receipt of certain licenses on behalf of the company. This investigation went on for several years. However, in 2013, the company announced that the DOJ had issued a declination to prosecute the company. Unfortunately, there is no specific information regarding this declination, either from DynCorp or the DOJ. DynCorp did state in its 10-K filing, "On February 5, 2013, the US Department of Justice notified us that their inquiry regarding this matter has been closed based upon a number of factors, including, but not

limited to, the voluntary disclosure by the company, the thorough investigation undertaken by the company, and the steps taken to enhance the company's anti-corruption compliance program."

Some guidance

So what does the DOJ look at when it reviews a company's FCPA compliance program with regards to facilitation payments? Initially, if there is a pattern of such small payments, it would raise a red flag and cause additional investigation, but this would not be the end of the inquiry. There are several other factors which the DOJ could take into account in making a final determination on this issue. The line of inquiry the DOJ would take is as follows:

1. Size of payment: Is there an outer limit? There is no outer limit but there is some line where the perception shifts. If a facilitating payment is over $100, you are arguing from a point of weakness. The presumption of good faith is against you. You might be able to persuade the government at an amount under $100. But anything over this amount and the government may well make further inquiries. Furthermore, the DOJ might say that all facilitation payments should be accumulated and this would be a pattern and practice of bribery.
2. What is a routine governmental action? Are we entitled to this action or are we asking the government official to look the other way on some requirement? Are we asking the government official to give us a break?
3. Does the seniority of the governmental official matter? This is significant because it changes the presumption of whether something is truly discretionary. The higher the level of the governmental official involved, the greater chance his decision is discretionary.
4. Does the action have to be non-discretionary? Yes, because if it is discretionary, then a payment made will appear to obtaining some advantage that is not available to others.
5. What approvals should be required? A facilitation payment is something that must be done with an appropriate process. The process should have thought and the decision made by people who are the experts within the company on such matters.
6. Risk of facilitation payments and third parties? Whatever policy you have, it must be carried over to third parties acting on your behalf or at your direction. If a third party cannot control this issue, the better compliance

practice would be to end the business relationship.

7. How should facilitation payments be recorded? Facilitation payments must be recorded accurately. You should have a category entitled "facilitation payments" in your company's internal accounting system. The labeling should be quite clear; they are critical to any audit trail so recording them is quite significant.
8. Monitoring programs? There must always be ongoing monitoring programs to review your company's internal controls, policies, and procedures regarding facilitation payments.

So, we return to the question of when does a grease payment become a bribe? There is no clear line of demarcation. The decision seems to turn on the amount of money involved, to whom it is paid, and the frequency of the payments. Additionally, accurate books and records are a must. Finally, there is the matter of burden of proof. Under trial court rulings in a dropped SEC enforcement effort against two individuals from Nobel Corp, Mark Jackson and William Ruehlen, it is incumbent on the SEC to negate any facilitation payment. Good luck with that if the government comes knocking. Any defendant who wishes to avail itself of this exemption better be ready to proffer credible evidence to support their position. Much like any compliance defense, it would be difficult to imagine that any company will want to use the facilitation payment exemption at any trial or other enforcement proceeding.

References

1. DiMauro, J., "New York Fed GC squeamish about grease payments", *The FCPA Blog*, 29 July 2014, see www.fcpablog.com/blog/2014/7/29/new-york-fed-gc-squeamish-about-grease-payments.html.

Chapter 12: Conclusion

I BEGAN my FCPA journey back in 2007 when I worked at a company which then had the largest FCPA fine in the history of the world, a whopping $27 million. Today, that amount does not even make the top twenty fines list. The explosion in FCPA enforcement has led directly to a large increase in fines and penalties. However, as great as the costs of the fines and penalties assessed by the DOJ or SEC might be, they are said to be generally less than the overall cost to a company who has to go through an enforcement action, I have heard that this figure can be two to six times the amount of the fines and penalties. Whatever that multiplier may be, it is certainly going to be costly to your organization.

If there is one thing that the DOJ and SEC have made clear, and this is backed up by all that I have learned in my own FCPA journey, it is that your only hope of avoiding some or most of these costs is by having an effective compliance program. While an effective compliance program will certainly be considered by government regulators when making a determination on whether to bring charges, having an effective compliance program will also provide your company with its best chance to stop a violation of your internal company policies and procedures before any actions become full-blown FCPA violations. That is certainly worth the cost of creating, implementing, and maintaining a compliance regime.

Above all, beyond all of the reasons listed above, having an effective compliance program makes good business sense. Companies with effective compliance programs tend to be better run. Moreover, private enterprise has responded to the increase in FCPA enforcement by implementing a business solution to legal issues raised by the increase in FCPA enforcement. If you want to represent a company on the sales side or enter into some other business

relationship, such as a JV, your company is going to be required to have a compliance program. If you want to supply a major multi-national company, your company will be required to have an effective compliance program. In other areas, anti-corruption compliance programs are becoming requirements to access cash to fund your business. If your company is going through traditional corporate refinancing in the next 18 months, any bank or other financial institution that you go to will want not only to review your compliance program, but may well want to review where that compliance program may be in terms of an overall assessment of the compliance risks that your company faces. If you want to sell your business or even receive some other type of funding, your compliance program will be assessed. Finally, if you want to have directors and officers' (D&O) insurance coverage for shareholder actions based on FCPA violations, your company will need to have a compliance regime.

Anti-corruption compliance enforcement is here to stay. That means, in today's business world, you will need to ensure effective anti-corruption compliance in almost any location where you do business, and at any entity you might choose to do business with going forward. An effective program should not be 100 paces past your company's internal financial controls. It may be five paces beyond where you are now. It is not difficult to institute and follow such a standard, but it does take commitment from senior management to lead and support the effort going forward.

Index

A

A.G. Lafley 69, 70, 71
Aaron Murphy 17
Adam Bryant 5, 6
Alcatel-Lucent SA 38
Amy Hutchens 27, 28
Andrew Baird 93
Andrew Ceresney 122
Anne Marie Logarta 19

B

Boris Groysberg 58
Brian Ching 64
Brooke Denihan Barrett 64

C

Carol Saint 49
Carol Switzer 14, 15, 17, 49, 51, 52, 53, 88, 99
Carola Hoyos 110
Cheryl Eckard 109
Christopher M. Matthews 109, 110
Clarissa Balmaseda 79

D

Daniel Biegelman 4, 54
Data Systems & Solutions LLC 131, 133

David Hildebrandt 113, 114
David Lawler 3, 39, 40, 42
David Stuart 26
Debbie Troklus 13
Deferred prosecution agreement 11, 12, 38, 79, 95, 96, 98, 119, 131, 133, 134
Department of Justice . . VIII, IX, X, 2, 11, 12, 14, 18, 19, 23, 26, 31, 37, 38, 42, 44, 49, 51, 63, 78, 79, 89, 93, 98, 110, 113, 114, 117, 118, 119, 122, 123, 125, 126, 131, 132, 134, 139, 140, 143
Diana Lutz 77, 99, 103
Dodd-Frank Act 72, 107
Donna Boehme 9, 24, 25

E

Emma Wollschlager Schwartz 13
Ethisphere 3

F

Fair process doctrine 71, 72, 111
FCPA . . . . . VII, VIII, X, XI, 1, 2, 9, 11, 12, 17, 18, 21, 23, 25, 26, 31, 32, 37, 38, 41, 42, 43, 44, 49, 51, 54, 55, 58, 62, 63, 64, 65, 66, 67, 68, 73, 77, 78, 80, 81, 83, 84, 85, 86, 88, 91, 93, 96, 97, 98, 99, 101, 102, 103, 104, 107, 108, 109, 110, 112, 113, 117, 118, 119, 123, 125, 126, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 143, 144
FCPA Blog 81, 137
FCPA Guidance . . . . . VIII, 1, 2, 11, 17, 18, 21, 25, 31, 37, 38, 44, 49, 51, 73, 78, 80, 93, 99, 107, 110, 117, 118, 123, 125, 126, 134, 137
Flora Francis 93
Foreign Corrupt Practices Act . . . . . VII, VIII, 17, 54, 78

G

Garth Peterson 18
GE Oil & Gas 93
GlaxoSmithKline PLC . . . . . VIII, 109
Greg Warner 13

H
Halliburton 2, 131, 132, 134
Human resources. 33, 66

I
Ian Foxley 110
Internal audit 14, 23, 33, 34, 41, 45, 49, 73, 99, 126, 127, 128
IT department 34, 109

J
Jaclyn Jaeger 35
James McGrath. 113, 114
James Nortz. 55, 56
Jay Martin 84, 91, 130
Jay Rosen. 22
Jimmy Lin 14
Joe Murphy 4
John Allen 17
Johnson & Johnson. 96, 131, 133
Jonathan Marks. 37
José Tabuena 108
JPMorgan Chase & Co. 63
Jules Goddard 7
Julian Birkinshaw 7
Justin Offen 120

K
Karen Kroll 77
Kendall Tieck 14
Kevin Ryan. 65

L
Lanny Breuer. 19
Larry Thompson. 3
Leonard Shen 45
Lou Casale. 109
Lynn Sharp 3

M

Marjorie Doyle *77*, 103
Martin Biegelman 4, 54
Mary Jones 96
Matt Kelly 66
Maxwell Technologies Inc. 38
McNulty's maxims 103, 104, 122, 123
Metcalf & Eddy. *37*
Michael Slind 58
Mike Paterson. 110
Mike Volkov 1, 9, 23, 41, *47*, *107*, 111
Morgan Stanley 18

N

Nathaniel Edmonds 125, 135
NCR Corp. 109
Non-prosecution agreement. 11

O

Opinion Procedure Release 08-02 . . . . . 131, 132, 134, 135
Opinion Procedure Release 10-02 89
Oversight Committee 100, 101

P

Panalpina 95, 96, 139
Paul McNulty 12, *70*, 103, 104, 122, 123
PepsiCo. 3
Pfizer 119, 131, 135, 136

R

Randy Colrey 81
Risk Advisory Group 91
Russ Berland. 114
Ruth Ward 19

S

Samuel Rubenfeld 109

Scott Moritz 79
Securities and Exchange Commission . . . . . .VIII, 2, 11, 12, 22, 26, 31, 37, 44, 51, 78, 79, 93, 110, 117, 118, 122, 123, 125, 126, 141, 143
Siemens. 2, 68
Society for Corporate Compliance and Ethics. 19, 24, 93, 112
Stephen Dubner 63
Stephen Martin 12, 29, 31, 104
Steven Levitt 63

T
Tammy Whitehouse 47
Tony Eccles 7
Tyco International 77, 79
Tyson Foods Inc. 38

U
UK Bribery Act . . . . . VIII, XI, 1, 2, 31, 32, 37, 38, 42, 49, 58, 78, 83, 84, 96, 98
UK Ministry of Justice 81, 84
UK Serious Fraud Office . . . . . VII, 78, 110
US Department of Justice. . . . . VIII, IX, X, 2, 11, 12, 14, 18, 19, 22, 23, 26, 31, 37, 38, 42, 44, 49, 51, 63, 78, 79, 89, 93, 98, 110, 113, 114, 117, 118, 119, 122, 123, 125, 126, 131, 132, 134, 135, 139, 140, 143
US Sentencing Guidelines. 1, 11, 23, 25, 26, 38, 51, 52, 67, 107

V
Van Halen 63
Victoria Ransom 5

W
Whistleblower 72, 107, 109, 110, 111
William Athanas 41