The continued evolution of best practices for compliance programs

Inside:
In 2019, the federal government released significant information which directly impacted compliance professionals. We cover all three releases in this ebook, the Evaluation of Corporate Compliance Programs - Guidance Document, the Framework for OFAC Compliance Commitments and the Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations.

AUTHORED BY:
Jonathan T. Marks, CPA, CFF, CFE
Partner, Firm Practice Leader - Global Forensic, Compliance & Integrity Services

Thomas R. Fox
The Compliance Evangelist
There were three significant releases of information by the federal government which directly impacted compliance professionals in 2019. Two came from the Department of Justice and one came from the Department of Treasury, Office of Foreign Asset Control. This eBook will discuss them all in depth and provide a structure for the compliance practitioner to use guidance from all three cases to implement best practices in their compliance program.

CONTENTS

3 I - Introduction
6 II - A well designed program
  8 ...... B. Policies & procedures
  10 ...... C. Training
  12 ...... D. Reporting & investigations
  14 ...... E. Third parties
  15 ...... F. M&A

17 II – Effective implementation
  17 ...... A. Commitment by senior & middle management
  19 ...... B. Autonomy & resources
  22 ...... C. Incentives & disciplinary measures

24 III – Does it work?
  24 ...... A. Continuous improvement, periodic testing & review
  27 ...... B. Investigation of misconduct
  28 ...... C. Analysis & remediation of any underlying misconduct

31 IV. What does at all mean?
  31 ...... A. Welcome to the OFAC compliance framework
  32 ............ Element 1 - Management commitment
  33 ............ Element 2 - Risk assessment
  34 ............ Element 3 - Internal controls
  36 ............ Element 4 - Testing and auditing
  37 ............ Element 5 - Training

38 V. The Antitrust Division guidance on an effective compliance program
  38 ...... A. Introduction
  39 ...... B. Elements of an effective Antitrust compliance program
  42 ...... C. Sentencing considerations
  44 ...... D. What does it mean for ABC compliance?

47 VI. Conclusion
51 Sources
52 About the authors
The criminal division’s evaluation of corporate compliance programs

In April, Assistant Attorney General Brian Benczkowski announced (ECI speech) an update to the 2017 Evaluation of Corporate Compliance Programs, which had been released in February 2017. This new document is entitled Evaluation of Corporate Compliance Programs - Guidance Document (2019 ABC Guidance) and is available for download at no charge. It should be mandatory reading for every Chief Compliance Officer (CCO), compliance practitioner and professional or any other person interested in the latest guidance from the Department of Justice (DOJ) on what constitutes a best practices compliance program. This white paper will discuss the 2019 ABC Guidance, identify differences and newly listed items from the 2017 Evaluation of Corporate Compliance Programs (2017 Evaluation), as well as provide insight on how the document should be used by compliance professionals who find themselves embroiled in a major compliance failure such as an investigation of a suspected violation of the Foreign Corruption Practices Act (FCPA). We will also consider how the compliance practitioner can use the document as a roadmap to develop and implement a best practices compliance program.

I - Introduction

The first thing to note is in the Introduction section, which lays out the purpose of the 2019 ABC Guidance. The 2019 ABC Guidance is designed to supplement the “Principles of Federal Prosecution of Business Organizations” published in Title 9 of the Justice Manual (formerly US Attorneys Manual) and provide assistance to prosecutors when reviewing their cases for potential criminal prosecution. The 2019 ABC Guidance states:

“This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation’s compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).”

This statement signifies the importance of having a best practices compliance program in place to help prevent, detect and remediate violations of laws such as the FCPA and what needs to be accomplished if a violation occurs.
The 2019 ABC Guidance goes on to emphasize the importance of a unique approach to evaluating any company’s corporate compliance program. It cites the use of a “rigid formula” to be inappropriate to make an assessment of the effectiveness of compliance programs. Rather, a tailored approach should be exercised when making determinations on a company’s compliance management.

“Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company’s risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case.”

Benczkowski emphasized during his speech at the ECI and during the informal Q&A afterwards, the flexible nature of this inquiry. Once again, the DOJ has clearly rejected the notion of a “one size fits all” approach. The reason is quite clear and straight-forward, with Benczkowski stating, “Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Department does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company’s risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case.”

The 2019 ABC Guidance then goes on to pose the following three “fundamental questions” that prosecutors must ask at the beginning of their analysis:

- “Is the corporation’s compliance program well designed?”
- “Is the program being applied earnestly and in good faith?” - In other words, is the program being implemented effectively?
- “Does the corporation’s compliance program work” in practice?

Benczkowski also explained how these three considerations assist in a prosecutorial analysis. First, prosecutors assess the adequacy and effectiveness of the corporation’s compliance program at the time of the offense, as well as at the time of a charging decision. This step helps guide the prosecutors in determining whether they should decline to bring a case, or, what a resolution would look like if it were appropriate for the matter under review.
This makes Benczkowski's declaration clear, that “there can be no question about the seriousness with which we take the effectiveness of a company's compliance program when determining whether and how to bring a corporate case.”

The next consideration in the analysis is a specific focus on a company's compliance program at the time of the misconduct which, if effective, could result in a significant reduction of the fine to be imposed. In addition, the FCPA shows mercy for companies that self-disclose, cooperate, and remediate to the extent necessary to reach a level considered effective. This mercy, which is based on the FCPA Corporate Enforcement Policy, calls for a 50% reduction in fines. When acting under these circumstances, Benczkowski explains that the fine prior to reduction is on the lower-end of the Sentencing Guidelines.

Further, the company's culpability score under the US Sentencing Guidelines determines the company's range for potential fines and penalties. This is important because if an entity has “maintained an effective ethics and compliance program at the time of the misconduct, the company would also be eligible for a significant reduction of its overall fine.” This means an overall fine would be further reduced based on the FCPA corruption Corporate Enforcement Policy (Policy), which provides for a 50% reduction off the low end of the Sentencing Guidelines in cases where the company has voluntarily self-disclosed, fully cooperated and fully remediated, which includes implementing an effective ethics and compliance program.

The third and final consideration the prosecutor makes in their analysis is whether or not the company's compliance program is “sufficiently effective to permit the company to self-monitor.” Specifically, “prosecutors look at the company's compliance program at the time of the resolution to determine whether an independent compliance monitor is necessary to prevent the reoccurrence of misconduct, or whether the compliance program is sufficiently effective to permit the company to self-monitor.” If the prosecutor determines this is not the case, an independent compliance monitor will be appointed to assist in facilitating the remediation process. This expands on the concepts laid out by Benczkowski when he published the Benczkowski Memo in the fall of 2018 which discussed the DOJ's use of corporate monitors going forward.

As we take a deeper dive into specifics of the 2019 ABC Guidance going forward, the comments made by Benczkowski at the ECI conference and the language in the 2019 ABC Guidance make clear to everyone that the DOJ has zero interest in using rigid formulas, such as ISO 37001, as a basis for some type of compliance defense. Companies must assess and manage their own risks and not simply follow a written checklist or paper program advocated by those still trying to append a compliance defense to violations of anti-bribery & corruption laws. Not only do these approaches fail in advancing the operationalization of compliance, but they also remove a key tool of prosecutorial discretion that rewards companies for meeting requirements to assess and manage risk.
II - A well-designed program

Next, we consider the first substantive section of the 2019 ABC Guidance, which focuses on the elements of a well-designed compliance program or as it states, “Is the corporation’s compliance program well designed?” Quoting from the Justice Manual, the 2019 ABC Guidance begins with the proposition, “The critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct.”

This leads directly to the starting point for all compliance programs - a risk assessment. The 2019 ABC Guidance further states that a prosecutor must begin by developing and understanding of the company’s business, the composition of its risk profile, and the integration of its compliance program to effectively “devote appropriate scrutiny and resources to the spectrum of risks.”

However, it does not stop with the performance of a one-time risk assessment. Risk assessments should be viewed as an iterative, ongoing process. On this point, the 2019 ABC Guidance emphasizes the importance of an individualized program, tailored to focus attention and resources areas of high risk. In other words, the company’s risk assessment and the compliance and ethics programs should overlap to provide special attention and resources to high-risk areas. The level to which these are effectively interlaced should be considered in the prosecutor’s analysis. This remains true even if the programs fall short in low-risk areas. The idea is the company was able to make an assessment, prioritize based on that assessment, and develop a compliance program with adequate coverage of the key risk areas identified.

“The critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct.”
A. Risk assessment

To accomplish all of this, the document sets out three broad standards:

**Risk management process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company’s compliance program?

The use of the phrase “risk management process” emphasizes it is not a one-off exercise but truly a process. As part of this process, the underlying methodology in determining, prioritizing and addressing risk must be substantiated and justified. Moreover, the DOJ has specifically focused on the metrics component of every risk assessment as a form of ongoing monitoring. This means it is not simply enough to have the metrics generated, they must be evaluated and communicated to those responsible for the compliance function.

**Risk-tailored resource allocation** – Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

This section focuses more intently on the true risks that each company faces and how you allocate your risk management resources to those risks. It mandates you to not only focus on mitigating your higher priority risks but more importantly recommends not wasting time and resources on low-risk areas. High-risk areas should be handled as such. For example, the use of third parties in the sales cycle presents a high level of risk and consequently, requires additional diligence and monitoring. If you use third parties as part of your company’s sales cycle, that may be the highest risk. Conversely, if your sales strategy is based on employees, then they may be your highest risk. The document also points out the explicit risks in specific transactions and with specific customers, including “large-dollar contract with a government agency in a high-risk country.” This example comes from several enforcement actions where the customer itself was not only involved in the bribery scheme but also facilitated the illegal transactions.

**Updates and revisions**

Is the risk assessment current and subject to periodic review? Have there been any updates to policies and procedures in light of lessons learned? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

This section mandates the nature of not only risk assessments but the continuous feedback loop of information both to and from your compliance program. Did you incorporate the information learned in the field into your next risk assessment? Did you then update your policies, procedures and controls around the information garnered from your updated risk assessment? The “OODA” loop in action. [Observe, Orient, Decide, Act]

All of this greater specificity in the entire risk management process is important guidance for every compliance practitioner. It also demonstrates that what was previously considered cutting edge just a few years ago is now considered a standard practice.
B. Policies and procedures

Policies and procedures are the backbone of every compliance program, and as you might expect, they play a significant role in the 2019 ABC Guidance. On this point, the 2019 ABC Guidance states, "Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations."

This point that the culture of compliance must be intertwined with day-to-day operations should not be taken lightly. It is one thing to have the policies and procedures written and in place. However, if staff is not aware of them or trained to act in accordance with them, they are more ornamental than effective.

**Design** – What is the company’s process for designing and implementing new policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

There are five general elements to a compliance policy, which should clarify the following: (1) Identify who the compliance policy applies to; (2) Establish the objective of the compliance policy; (3) Describe why the compliance policy is required; (4) Outline examples of both acceptable and unacceptable behavior under the compliance policy; and (5) Advise on the specific consequences for failure to comply with the compliance policy.

**Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

There are numerous reasons to put some serious work into your compliance policies and procedures. They are certainly a first line of defense when the government comes knocking. The regulators will take a strong view against a company that does not have well thought out and articulated policies and procedures; all of which should be systematically reviewed and updated.
Accessibility – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees’ access?

If there was ever any doubt, it is now clear that your compliance policies and procedures must be translated into local language for your non-English speaking workforce. The key is that your employees have the same understanding of the compliance policies and procedures, no matter the language. It is also important to ensure the essence of the policies and procedures as crafted are captured in the translated versions. If you’re not careful, it’s easy to lose meaning in translation.

Responsibility for operational integration – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees’ understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company’s internal control systems?

This means more than simply having appropriate policies and procedures. It also includes operationalizing them into your compliance program, down to the business unit level, but how can you do so? Compliance training is only one type of communication. This is a key element for compliance practitioners because if you have a 30,000+ global workforce, the simple logistics of training can appear daunting. The use of smaller groups, where detailed questions about policies can be raised and discussed, can be a powerful teaching tool. Another useful learning technique includes posting Frequently Asked Questions (FAQs) virtually and in common areas within the company. Additionally, requiring employees to sign written compliance policies provides what some consider the most vital method of communication. A simple acknowledgement leaves no room for ignorance as an excuse when policies and procedures are violated.

Gatekeepers – What, if any, guidance and training has been provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

If you consider training as one source of your organization’s 360-degrees of compliance communications, the rollout of a new or updated code of conduct can be another opportunity. This rollout fits directly into the concept of 360-degrees of compliance, as it is an integral part of both communications and engagement. How have you trained your middle managers to listen in a speak up culture? Where do they report concerns? You will need to have a protocol in place to document this area.

Given the number of ways that information about violations or potential violations can be communicated to government regulators, having a robust scoping or triage system is an important way that a company can determine what resources to bring to bear on a compliance problem.
C. Training

Next, consider the DOJ’s specific focus on effective training. On this point, the 2019 ABC Guidance states, “Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.” Training is a key component of developing a culture of compliance. Good policies and procedures are not useful if they are not communicated to those responsible to abide by them.

**Risk-based training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

This requires you to assess your employees for risk to determine the types of training you might need to deliver. This means that you should risk rank your employees. It is highly likely the sales force would be the highest risk but there may be other employees deserving of high-risk training as well. From your risk ranking, you need to then develop training tailored for the risks those employees will face. The key going forward is that you have thoughtfully structured your compliance training program, not only in the design but also in the delivery which, is combined with backend periodic review and determination of effectiveness of the program elements.

**Form/Content/Effectiveness of training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company’s rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed employees who fail all or a portion of the testing?

One of the key goals of any anti-bribery & corruption compliance program is to elevate employee awareness and understanding of applicable anti-bribery & corruption laws and regulations; your specific company compliance program; and to create and foster a culture of compliance. Beginning in the fall of 2016 through the announcement of the FCPA enforcement Pilot Program, the DOJ began to discuss whether or not defendants have determined the effectiveness of your training. This continued with the release of the 2017 Evaluation where they asked, “How has the company measured the effectiveness of the training?” and has now been brought forward in the release of the 2019 ABC Guidance. It is a key metric for the government to use when evaluating compliance training programs.

Here you could look to the example of Shawn Rogers, the Senior Director, Global Ethics and Compliance - Training and Awareness at Walmart. While he was the Lead Counsel of Compliance Training and Communications at General Motors (GM), he set up a more formalized corporate governance structure to look at required training. He and his peers assigned key players from executive and management roles to function as project heads. This allowed the different disciplines to participate in the course development process. The charter he and his team set in place lists their scope of responsibility. It allowed GM to more fully document its rationale for training.

The bottom line is that it is about (a) training the right people, (b) training them on the right risk, (c) getting to the right level of detail, and (d) training them in the proper language (linguistic and institutional). He also mentions the importance of training frequency and, notably, modelling realistic risk situations for better employee preparedness to respond to compliance risks.
Communications about misconduct – What has senior management done to let employees know the company’s position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company’s policies, procedures, and controls (e.g., anonymized descriptions of the type of misconduct that leads to discipline)?

This requirement is more than simply the ubiquitous “tone-at-the-top,” as it focuses on the communications of senior management. The DOJ wants to see a company’s senior leadership communicating about not only compliance successes but also compliance failures and how they can be used as lessons learned going forward. The DOJ asks if company leadership has, through their words and concrete actions, communicated the right message of doing business ethically and in compliance with applicable laws and regulations.

Availability of guidance – What resources are available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

Here, we suggest you consider a 360-degree view of compliance communication to incorporate your compliance identity into a holistic approach so that compliance is in touch with and visible to your employees at all times. It is about creating a distinctive brand philosophy of compliance which is centered on your consumers. In other words, it helps a compliance practitioner to anticipate all the aspects of your employees needs around compliance. A 360-degree view of compliance gives you the opportunity to build a new brand image for your compliance program.

Moreover, the 360-degree approach allows you to monitor your compliance communication activities by tracking attendance at events, monitor website statistics, quantify open rate of emails, downloads of materials, video hits; in other words, the same techniques that your marketing team uses to determine the effectiveness of their messaging. The objective is to build trust for the 360-degree process by determining if the goal was achieved. You can utilize surveys or focus groups to assess the impact on your target audience. By focusing on your customers of compliance (i.e., your employees), it allows you to identify gaps and improve the communication process for your compliance program.

A: Train the right people
B: Train them on the right risk
C: Get to the right level of detail
D: Train them in the proper language
D. Reporting and investigations

On reporting and investigations, the 2019 ABC Guidance states, “Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company’s code of conduct, company policies, or suspected or actual misconduct. Prosecutors should assess whether the company’s complaint-handling process includes pro-active measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company’s processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.”

The implementation of this mechanism and related follow-up processes are of incredible importance for a company’s compliance culture. If employees don’t feel as though they have a place to report their concerns, and that something will be done with the information they’ve reported, there is a barrier in their ability to trust their working environment.

**Effectiveness of the reporting mechanism** – Does the company have an anonymous reporting mechanism, and, if not, why not? How is the reporting mechanism publicized to the company’s employees? Has it been used? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

Internal reporting mechanisms have become not only more important in the #MeToo era but also more useful in reducing both costs and legal exposure to companies. The 2018 ACFE Report to the Nations – Global Study on Occupational Fraud and Abuse cites that tips are the most common method to initially detect fraud schemes in an organization. Tips came in at 40% compared to internal audit, 15%; and management review, 13%. Moreover, this requirement is more than simply maintaining hotlines. Companies have to make real efforts to listen to employees. You need to have managers who are trained on how to handle employee concerns; they must be incentivized to take on this compliance responsibility and you must devote communication resources to reinforcing the company’s culture and values to create an environment and expectation that managers will raise employee concerns.

**Properly scoped investigations by qualified personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?
Given the number of ways that information about violations or potential violations can be communicated to government regulators, having a robust scoping or triage system is an important way that a company can determine what resources to bring to bear on a compliance problem. Jonathan Marks, a partner at Baker Tilly Virchow Krause, LLP, has articulated a five-stage triage process which allows for not only an early assessment of any allegation, but also an organized structure to think through your investigative approach. But more than simply scoping the information, you must have an experienced investigator or other seasoned professional making these determinations, if not a more well-rounded group or committee. Next, what will be the types of evidence to consider going forward? Finally, before selecting a triage solution, understand what tools are available, including both forensic and human, to complete the investigation.

**Investigation response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

Your company should have a detailed written procedure for handling any complaint or allegation of bribery or corruption, regardless of the means through which it is communicated. The mechanism could include the internal company hotline, anonymous tips, or a report directly from the business unit involved. You can make the decision on whether or not to investigate with consultation with other groups such as the Audit Committee of the Board of Directors or the Legal Department. The head of the business unit in which the claim arose may also be notified that an allegation has been made and that the Compliance Department will be handling the matter on a go-forward basis. Through the use of such a detailed written procedure, you can work to ensure there is complete transparency on the rights and obligations of all parties once an allegation is made. This allows the compliance team to have flexibility and assigned responsibility to deal with such matters, from which it can best assess and then decide on how to manage the investigation.

**Resources and tracking of results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses?

The investigation will be critical for you to help understand what remediation your compliance program will need going forward, since it is likely that an employee or outsider has identified a way to override your control system. Conversely, are there issues in the overall executive tone, governance, compliance program or internal control framework which failed? You cannot find gaps in your compliance system until you stress test it. In this light, your compliance failures can be viewed as the ultimate stress test. Your investigation should ideally show where the system broke down. The investigation will identify information to you about the failures of your compliance program that you may not have known existed previously. This requirement mandates that you use the information uncovered in your investigation to not only remediate the issue at hand, but to use the information on a proactive basis going forward.
E. Third parties

Third-parties are still recognized as one of the very top risks under the FCPA. On this point, the 2019 ABC Guidance states, “A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the degree of appropriate due diligence may vary based on the size and nature of the company or transaction, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions. Prosecutors should also assess whether the company knows its third-party partners’ reputations and relationships, if any, with foreign officials, and the business rationale for needing the third party in the transaction.” The guidance also emphasizes the importance of the company’s ongoing monitoring of third party relationships. It is not something that should be done once and forgotten. Rather, there should be a process in place for ongoing monitoring of these business relationships “be it through updated due diligence, training, audits, and/or annual compliance certifications by the third [parties].”

Risk-based and integrated processes – How has the company’s third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

By linking contractual compensation to performance, there should be an increase in third-party performance. This is especially valuable when agreed upon key performance indicator (KPI) metrics can be accurately measured and tracked. This would seem to be low hanging fruit for the compliance practitioner. If you cannot come up with some type of metric from the compliance perspective, you can work with your business relationship team to develop compliance KPIs.

You should rank third parties based upon a variety of factors including performance, length of relationship, benchmarking metrics and KPIs. This will allow for the compliance practitioner to have an ongoing risk ranking of its third parties that can work as a preventative and even prescriptive, prong of a compliance program. By appropriately risk ranking your third parties, the company will be able to effectively allocate compliance resources to those third parties that warrant them.

Appropriate controls – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?
This step is broken into two parts: business sponsor and business justification. The purpose of the business justification is to document 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. It is mandatory this document be completed, in full, by the business sponsor, who will be the primary contract with the third-party for the life of the business relationship. The business sponsor will also be your key first line to document that the contracted services have been performed.

Management of relationships – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third-party relationship managers about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties?

One of the key elements for any third-party contract is the compensation issue. If the commission rate is too high, it could create a very large pool of money that could be used to pay bribes. It is mandatory that your company link any commission or payment to the performance of the third-party. If you have a long-term stable relationship with a third-party, you can tie compensation into long-term performance, including long-term compliance performance. This requires the third-party to put “skin into the compliance game” so that they have a vested, financial interest in accomplishing their goals in accordance with applicable laws and regulations.

F. M&A

On the issue of mergers & acquisitions (M&A), the 2019 ABC Guidance stated, “A well-designed compliance program should include comprehensive due diligence of any acquisition targets. Pre-M&A due diligence enables the acquiring company to evaluate more accurately each target’s value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete due diligence can allow misconduct to continue at the target company, causing resulting harm to a business’s profitability and reputation and risking civil and criminal liability. The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.”

Due diligence process – Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

The DOJ has consistently emphasized the pre-acquisition phase and the 2019 ABC Guidance took a deeper dive into their expectations. The guidance emphasizes the need for the compliance component of your M&A regime to begin with a preliminary pre-acquisition assessment of risk. Such an early assessment will assist in the transaction research and evaluation phases. The preliminary assessment 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 to be used in the diligence process. From this document, you should be able to prepare a focused series of queries and requests to be obtained from the target company. Thereafter, management can use this pre-acquisition risk assessment to attain what might be required in the way of integration, post-acquisition. It is also a helpful tool to inform the corporate and business functions of how they may be affected as a result of the purchase, from a practical, monetary and cultural perspective. These costs are not insignificant, and they should be thoroughly evaluated in the decision-making calculus.
**Integration in the M&A process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

This is a new inquiry. While many companies have post-acquisition integration as one of the functions of a corporate compliance program, many have yet to move compliance into the pre-acquisition phase. The DOJ is making it clear, yet again, that compliance needs to be a part of your company’s M&A strategy throughout the entire process. Moreover, from the business perspective, it is much more cost-efficient and timely to involve your corporate compliance function in the pre-acquisition phase. The anti-bribery & corruption enforcement world contains many examples of enforcement actions involving companies which did not include compliance as part their M&A team and this gap allowed bribery and corruption schemes and risks to continue after the transaction closed.

**Process Connecting Due Diligence to Implementation** – What has been the company’s process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company’s process for implementing compliance policies and procedures at new entities?

The bottom line is that you must train employees of the newly acquired company, reevaluate third parties under your company’s standards, and conduct compliance audits on new business units. This process should be based on your pre-acquisition due diligence and compliance risk assessment. Moreover, the 2019 ABC Guidance clearly views both the pre- and post-acquisition phases of M&A as tied together in a unidimensional continuum. If pre-acquisition due diligence is not possible, you should review the requirements and time frames laid out in Opinion Release 08-02 or the 2012 FCPA Guidance, which noted, "pursuant to which companies can nevertheless be rewarded if they choose to conduct thorough post-acquisition FCPA due diligence." Whatever steps you utilize for post-acquisition integration, they should be taken as soon as is practicable.

The earlier you can deploy these steps, the better off your company will be at the end of the day. A merger or other acquisition that fails for compliance reasons is a preventable disaster of the first order. One need only consider the Latin Node Inc. FCPA enforcement action where the acquiring company had to write off its entire investment because it had wholly failed to engage in appropriate pre-acquisition due diligence. Equally important to the costs of a potential FCPA violation(s) are the benefits to following this prescription from the 2019 ABC Guidance in light of the Safe Harbor for M&A announced in July 2018.

In order to extract from the real incentives and benefits the DOJ offers companies under the Policy, the company should engage in pre-acquisition due diligence, coupled with post-acquisition auditing, remediation, reporting and compliance program integration and training, it is clear the DOJ is once again demonstrating real incentives for companies to come forward and benefit from the Policy. In light of the ABC Guidance, there will be a presumption of a declination, not simply the language from the 2012 FCPA Guidance which states that the DOJ "may" grant a declination.

This clarification highlights two key components of the Policy and 2019 ABC Guidance: incentives and clarity. Companies are now highly incentivized to present evidence of FCPA wrong-doing as the benefits are now more clear. This is even more significant in the M&A context. If a company purchased a business, not previously subject to the FCPA and that target had engaged in bribery and corruption; it is not the previous owner who is at risk of violating the FCPA going forward, but your company. This reason alone provides a powerful incentive for companies to root out any corruption in the post-acquisition phase and that incentive has been clearer documented in the 2019 ABC Guidance going forward.
II – Effective implementation

The second fundamental question asked in the 2019 ABC Guidance is “Is the program being applied earnestly and in good faith?” In other words, is the program being implemented effectively? Moving logically from the starting point of compliance program design, you next need to determine if your compliance program is effective. This is the key step missed by those who advocate for the paper program of a compliance defense. For it is not simply having a compliance program in place but making sure it is effectively implemented that is the key to the prevention, detection and remediation of issues when they arise.

Nailing this final point directly, the 2019 ABC Guidance states, “Even a well-designed compliance program may be unsuccessful in practice if implementation is lax or ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a “paper program” or one “implemented, reviewed, and revised, as appropriate, in an effective manner.”

In addition, prosecutors should determine “whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts.” Prosecutors should also determine “whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it.”

A. Commitment by senior and middle management

Obviously, it all begins at the top, including the Board of Directors and most specifically senior management. The 2019 ABC Guidance states, “The company’s top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company’s ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them.” The compliance roles of the board of directors, senior management and middle management are all unique, but are focused on accomplishing the same goals. The three must work together in their different functions in order to maintain a full-spectrum compliance culture. To assist companies in understanding this requirement, the 2019 ABC Guidance sets out the following inquiries.

Conduct at the top – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

This requirement is more than simply the ubiquitous “tone-at-the-top,” as it focuses on the conduct of senior management. The DOJ wants to see a company’s senior leadership actually engaged in compliance and walking the walk. The DOJ asks if company leadership - through their words and concrete actions - brought the right message of doing business ethically and in compliance. How does senior management model its behavior after the company’s stated values and, finally, how is such conduct monitored in an organization?

This means you must document corporate decisions where a proposed compliance solution was rejected by management. In other words, is there a business justification for moving forward with the action or activity even after the compliance function recommended an alternative course of action. If the action or activity occurs, how was the compliance risk mitigated by the organization? Additionally, the compliance techniques or controls used to mitigate the risk should be documented to demonstrate that your compliance function employed the appropriate steps to reduce the overall risk.
Shared commitment – What actions have senior leaders and middle-management stakeholders (e.g., business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives? This requirement speaks to the greater role of non-compliance functions in a fully operationalized compliance program. Indeed, one sign of a mature anti-bribery & corruption compliance and ethics program is the extent to which a company’s other corporate disciplines are involved in implementing and then administering a compliance solution. This approach can act as a lynchpin in spreading a company’s commitment to compliance throughout the employee base. It can also be used to ‘connect the dots’ for many divergent elements of a corporate compliance and ethics program.

Even more important is the operationalization of compliance into the fabric of the business. One of the key indicia of compliance program effectiveness is how thoroughly each separate corporate discipline incorporates compliance into its everyday job functions. An active and functioning compliance program will literally be alive in each department in an organization.

By having as many touchpoints as possible with other corporation functions, a corporate compliance program moves downward and outward through the organization. Each one of these touchpoints can be used to teach, educate and reinforce the message of conducting business ethically and in compliance with relevant anti-bribery & corruption laws.

Oversight – What compliance expertise has been made available to or is present on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

This series of questions portends more than simply a reporting requirement, or that the CCO has a direct line to the Board. It is a separate requirement for the presence of compliance expertise on the Board. A review of any of the most recent corporate scandals; Wells Fargo, Uber Technologies, Volkswagen, Equifax, shows a complete lack of compliance expertise on the Board. The presence of a seasoned compliance professional on the Board is now enshrined as a best practice for companies. The DOJ may soon expect there to be a Compliance Committee separate and apart from the Audit Committee.

Finally, it is important that the Board receives direct access to such information on a company’s policies on this issue. The Board’s Audit Committee or Compliance Committee must receive quarterly reports from the CCO. Your Board should create a Compliance Committee as the Audit Committee may more appropriately deal with financial audit issues. A Compliance Committee can devote itself exclusively to non-financial compliance matters such as fraud, employee misconduct or other alleged violations of laws, regulations and/or company policies. The Board’s oversight role should include receipt of regular reports on the structure of the company’s compliance program, actions taken, and self-evaluations related to the effectiveness of the program. The Board can use this information to provide oversight of managing risk to making modifications to the compliance program. The requirement also means the Board must actually actively engage in the oversight role and not simply receive quarterly reports from the CCO. Has the Board separately tested the compliance function or even taken a deeper dive into a specific area of risk?
B. Autonomy and resources

Beginning with the 2016 FCPA Pilot Program, the DOJ began talking more and more about this issue in the context of the Chief Compliance Officer’s expertise, compensation and promotability within an organization. There also began a more robust examination of compliance function expertise, funding and head count. These points were further refined in the FCPA Corporate Enforcement Policy. In the 2019 ABC Guidance, there is further clarification from the DOJ. The 2019 ABC Guidance states, “Effective implementation also requires those charged with a compliance program’s day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured.

Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board’s audit committee. Each analysis will be different as every company is different. The key here is that for a compliance program “to be truly effective, compliance personnel must be empowered within the company.”

The 2019 ABC Guidance mandates further there should be an evaluation of the internal audit function in an oversight role to ascertain if the compliance function is “in fact empowered and positioned to effectively detect and prevent misconduct.” The compliance resource issue is expanded beyond the funding and head count to actual expertise within the function itself and on the Board. This means you must do more than simply give your General Counsel the CCO title; that role must have real compliance expertise.

Structure – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive within the company, and does that person have other roles?

It is important that the Board receives direct access to such information on a company’s policies on this issue. The Board’s Audit Committee or Compliance Committee must receive quarterly reports from the CCO. Your Board should create a Compliance Committee as the Audit Committee.
within the company? Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place?

How is your compliance function designed and structured? Is your compliance function housed in the legal department, in internal audit, another corporate function or housed separately? Where does compliance report to and is there unfettered access to the Board? As with most concerns in a compliance program, you must find a structure that works for your organization. Yet what you must fulfill under these questions is to have a thoughtfully created structure that meets these obligations. You must be able to articulate why you have chosen structure that meets the subject matter and technical expertise of a best practices compliance program.

**Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company’s strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

These factors dovetail into several areas posed in the FCPA Corporate Enforcement Policy. The DOJ is seeking real information around CCO and compliance function authority. You will need to demonstrate (1) the quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk; (2) The authority and independence of the compliance function and the availability of compliance expertise to the board; (3) The compensation and promotion of the personnel involved in compliance, in view of their role, responsibilities, performance, and other appropriate factors; and (4) The reporting structure of any compliance personnel employed or contracted by the company.

**Experience and qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? Who reviews the performance of the compliance function and what is the review process?

Clearly the DOJ is articulating that it expects true compliance professionals, who understand the way compliance interacts with and supports the business. The days of a law school trained CCO who cannot read a spreadsheet are consigned to the dustbin of non-compliant history. But more than simply compliance professionalism, companies must compensate and promote compliance professionals within their organization. Simply assigning someone to the compliance function of a law department because they cannot perform others roles within the company will no longer suffice.

Moreover, how does your organization assess its compliance function? Is there a full 360-degree review of the compliance team and its role, in addition to the internal audit requirements previously articulated? Is this assessment done in-house or by an independent third-party? Are these results made available to senior management and the Board of Directors?

**Funding and resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

You will now have to justify your corporate compliance spend. This means at a minimum you will have to meet some general industry standard. If a corporation tries to minimize compensation for compliance professionals, as well as the functions budget and personnel assigned to the function, it will not be viewed positively by government agencies. Also noted in the 2017 Evaluation, a company must be prepared to defend any denials of requests for compliance resources. Budget requests and allocations are always difficult times in any corporation. There is never enough money to go
around and most senior management thinks it is their job to slash all budget requests as a simple matter of course. Now such blanket management will be penalized.

If a compliance function is so hampered by resource restrictions it cannot carry out the basic functions needed for a compliance program to operate, it will not find favor under either the 2017 Evaluation or the Anti-Bribery & Corruption Corporate Enforcement Policy. If there are compliance projects needed to address basic compliance risks which are not funded because management failed to heed a CCOs or compliance functions budget request, this could be evidence of conscious indifference by senior management. The bottom line is the DOJ is focusing more on the role, expertise and how the compliance function is treated within an organization. This series of questions relates to compliance department funding and head count, down to the tactical level of how much is the CCO paid. What is the number of persons in working in your operationalized compliance function? You must also be able to justify the compliance budget so if you pay your CCO considerably less than your GC, you may now be required to explain and or justify that the disparity in compensation. If you maintain a Legal department budget of five million dollars and the budget for the compliance department is $500,000; you may be starting behind the 8-ball.

**Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

The DOJ has not taken a position on whether a GC can also be the CCO. It also signals the larger issue that the CCO should have a separate reporting line to the Board, distinct and apart from the GC. While the DOJ’s stated position that it does not concern itself with whether the CCO reports to the GC or reports independently, it is more concerned about whether the CCO is able to speak directly to the CEO or Board of Directors without input or restrictions imposed by the GC. Even if the answer were yes, the DOJ would want to know if the CCO has ever exercised that right. Yet the 2017 Evaluation comes to articulating a DOJ policy that requires that the CCO be independent of the GC’s office. Therefore, if your CCO still reports up through the GC, you must have demonstrable evidence of both CCO independence and actual line of sight authority to the Board.

Here are some questions you should consider in evaluating the effectiveness of the CCO’s reporting lines. First and foremost, is the CCO a part of senior management or the C-Suite? Does the CCO participate in regular meetings of this group? Who can terminate the CCO - is it the CEO, the Board Compliance Committee or does CCO termination require approval of the entire Board? Most importantly, could a person under investigation or even scrutiny by the CCO fire the CCO? If the answer is yes, the CCO clearly does not have requisite independence.

**Outsourced compliance functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed? This is one area where the DOJ has expanded its inquiry significantly. As the outsourcing of this function has increased from the business perspective, many companies have failed to engage in appropriate oversight and monitoring of the outsourcing company. Of course, organizations outsource their compliance function largely because (1) cost issues and (2) lack of expertise. Companies with outsourced compliance programs usually do not have either the money, time, inclination or ability to adequately oversee the outsourced compliance work.

While outsourcing might make sense from a cost perspective, it can be largely problematic if it is not managed properly. Rarely do outsiders have the same access as corporate employees, particularly in a function as important as compliance. Additionally, there will never be a level of trust with outsiders like there is with someone who wears the same color shirt as the employees. Here a company must not only have a rationale in place, which will largely be cost-savings; a company must also have a mechanism in place to assess, on an ongoing basis, any outsourced compliance function.
C. Incentives and disciplinary measures

Another key element of effective compliance program is the establishment of incentives for compliance and disincentives for non-compliance. This was laid out in the 2012 Resource Guide in Hallmark V of the Ten Hallmarks of an Effective Compliance Program and has been further discussed by the DOJ since that time. This carrot and stick approach requires punishment for problematic behavior and rewards for exemplary behavior. The 2019 ABC Guidance mandates that "Prosecutors should assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company’s communications convey the message that unethical conduct will not be tolerated and will result in swift consequences, regardless of the employee's position or title.

**Human resources process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? Is the same process followed for each instance of misconduct, and if not, why? Are the actual reasons for discipline communicated to employees? If not, why not? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

This prong requires rigor and process around your disciplinary program. It also requires objectivity in your disciplinary process. That objectivity is called the Fair Process Doctrine, which recognizes that there are fair procedures, not arbitrary ones, used during the process of disciplining employees. 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. As you incorporate the Fair Process Doctrine in your compliance program, you will meet the requirements under the 2019 ABC Guidance in the area of administration of discipline.

One of the areas which Human Resources (HR) can operationalize your compliance program is to ensure that discipline is handed out fairly across an organization and to reward those employees who integrate such ethical and compliant behavior into their individual work practices. In addition to providing a financial incentive for ethical behavior, it also provides a sense of institutional objectivity, which originates from procedural fairness and is one of the things that will bring credibility to your compliance program.

**Consistent application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Are there similar instances of misconduct that were treated disparately, and if so, why?
The above prong required objectivity in your disciplinary process. Discipline must not only be administered fairly but it must be administered uniformly across the company for the violation of any compliance policy. If you are going to fire employees in South America for lying on their expense reports, you have to fire them in North America for the same offense. It cannot matter that the North American employee is a friend or a so-called “high performer.” Failure to administer discipline uniformly may destroy any vestige of credibility that you may have developed up until that point.

Incentive system – Has the company considered the implications of its incentives and rewards on compliance? How does the company incentivize compliance and ethical behavior? Have there been specific examples of actions taken (e.g., promotions or awards denied) as a result of compliance and ethics considerations? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel?

While your sales compensation program can incentivize the achievement of sales and revenue targets, the program must expand beyond simple financial formulas. The compensation program must include elements to incentivize the goals of your compliance program. This may mean that you may need to change the incentives as the compliance programs matures; from installing the building blocks of compliance to integrating anti-corruption compliance within the DNA of your company.

There are three key questions you should ask yourself in modifying your compensation structure. First, is the change simple? Second, is the changed aligned with your company values? Third, is the effect on behavior immediate due to the change?

Incentives can be integrated into the DNA of a company through the hiring and promotion processes. There should be a compliance component to all senior management hires and promotions up to the highest levels within a company. Human Resources can provide strong support to design an effective compensation structure with consideration of including goals to align with the companies compliance program. Employees are well aware of those coworkers receiving promotions as well as the reasons for these promotions. Employees receiving promotions for achieving their sales targets in an unethical or unscrupulous manner will set a bad example for everyone and may in fact incentive bad behavior within the organization.

The DOJ provided some guidance related to this series of questions. The 2019 ABC Guidance stated, “some companies have found that publicizing disciplinary actions internally, where appropriate, can have valuable deterrent effects. At the same time, some companies have also found that providing positive incentives – personnel promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership – have driven compliance. Some companies have even made compliance a significant metric for achieving management bonuses and/or have made working on compliance matters or within the compliance functions a means of career advancement.”
III – Does it work?

The third and final fundamental question asked in the 2019 ABC Guidance is “Does the corporation’s compliance program work in practice?” This final section focuses on your ongoing monitoring and two other areas specific to anti-bribery & corruption compliance: third-parties and mergers and acquisitions (M&A). Admittedly, “one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.” Yet it is companies which need to prepare to answer this difficult question if they find themselves in the throes of an anti-bribery & corruption investigation. The 2019 ABC Guidance made clear that simply because there is an issue or even a FCPA violation, it does not “mean that a compliance program did not work or was ineffective at the time of the offense.” After all it is people who operate in the corporate environment and those people sometimes make bad decisions or act in their own self-interest despite the presence of a compliance program. However, if a corporate compliance program does effectively identify misconduct, “including allowing for timely remediation and self-reporting, a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively.”

This means that “in assessing whether a company’s compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company’s remedial efforts.” This message was driven home by Benkowczi during his speech at the ECI Conference whereupon he stated, “Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Department does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company’s risk profile and solutions to mitigate these risks warrant particularized evaluation. Accordingly, we make an individualized determination regarding the effectiveness of a corporate compliance program in each case.”

To fulfill this mandate, 2019 ABC Guidance specifies, the DOJ will “determine whether a company’s compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.”

A. Continuous improvement, periodic testing and review

Even with a well-designed program, which has been implemented effectively, your work is not done. This is because the business world is incredibly dynamic and your risks are constantly evolving. New markets, new services and new business opportunities can all create new risks. When you overlay the regulatory and legislative change, not simply in the US but literally across the world for a global entity, you can see the need for not only ongoing monitoring and review but updating as necessary. Here one only need to consider the latest wave of corruption cases not simply involving foreign government officials but the customers themselves. Further, as companies become more sophisticated in their compliance controls, the bad guys are getting equally sophisticated in the techniques to defraud companies into creating pots of money to pay bribes.

All of this means that for a compliance program to remain effective it must have a capacity to improve and evolve. The 2019 ABC Guidance states, “prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company’s size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider how you incorporated lessons learned into your compliance programs. This includes lessons learned from internal monitoring but also lessons learned from other
As a matter of course, you should audit the compliance program in your own organization. This type of audit should include the identification and analysis of accounting and internal-controls present within your organization.

compliance programs. Obviously, enforcement actions involving companies in your industry are a valuable source of information but here your lessons can literally come from any source. Prosecutors should likewise look to whether a company has taken reasonable steps to ensure your compliance and ethics regime is followed, including ongoing monitoring, testing and auditing to detect illegal and unethical conduct. Finally, every compliance program should be periodically evaluated to test the effectiveness of your compliance program.

**Internal audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

Your internal audit function is a critical part of your compliance regime. Auditing can take several different forms in an anti-compliance program. As a matter of course, you should audit the compliance program in your own organization. This type of audit should include the identification and analysis of accounting and internal-controls present within your organization. This information can be used to produce a fact-based report that can inform the decision-making process during inquiries, investigations and dispute resolution. The by-products of a forensic audit may also include remediation strategies to help a company mitigate and remedy procedural or internal-controls gaps that allowed the underlying issue to occur. Further, an internal audit can review a compliance process to determine if employees are following prescribed processes or internal controls.

In addition to the identification and analysis of evidence, an auditor’s objective is to attest to the credibility of assertions that are under examination, such as the material accuracy of financial statements for which the audited company’s management is responsible. Obviously one of the functions of such an audit is to determine if further investigation is warranted if there are red flags of possible fraudulent financial statements or misrepresentations made in the books and records of the organization. Once again, this dichotomy points out the difference between having a paper compliance program in place and a program that is actually performing as designed.
Your audits should be focused on your organization’s high-risk areas, both in terms of potential risks of bribery in corruption but also deficiencies in your internal controls and even consideration of your organization’s culture. Last, but certainly not the least, is how your organization uses the results of the audit. The results should be incorporated into enhancing your compliance program and remediating any deficiencies as well as conducting a root cause analysis to determine what caused the deficiencies.

**Control testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third-parties does the company undertake? How are the results reported and action items tracked? One of the key components of your internal audit protocol should be to test your compliance internal controls. This means that if you have a multi-country or business unit organization, you need to determine how your compliance internal controls are inter-related up and down the organization. This control testing should reflect this business reality. Finally, if your company relies heavily on technology for your compliance function, you can leverage that technology to “support the ongoing assessment and evaluation” program going forward. A four-step approach can be used to think through this requirement. (1) You should make an overall assessment of your company’s system of compliance internal controls to determine whether the controls are operating together in an integrated manner. (2) Take a deeper dive down into more thoroughly reviewing any of your controls found to have deficiencies and determining whether there are any compensating compliance internal controls. (3) Next, move to the assessment step to determine if your compliance internal controls is present and functioning. The goal is determine the existence and potential severity of any deficiencies. (4) Finally you should summarize the results so they can be remediated on a structured basis.

**Evolving updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

One of the critical elements found in the 2019 ABC Guidance is the need to use the information you obtain, whether through risk assessment, root cause analysis, investigation, hotline report or any other manner to remediate the situation which allowed it to arise. This is continuous improvement and there are three types of continuous improvement: 1) internal audit, 2) control testing, and 3) evolving updates; each category was further refined with multiple attendant questions.

The 2019 ABC Guidance mandates that your organization use a gap analysis. This is a method of assessing the differences in performance between a business’ internal controls to determine whether business requirements are being met and, if not, what steps should be taken to ensure they are met successfully. Moreover, it is a determination of the degree of conformance of your organization to the requirements of an internal controls standard. A gap analysis is mainly a document review or a “show me the evidence” type of activity, evidence which usually will come in the form of a record or document. There may be some audit steps used during a gap analysis as key stakeholders are asked to provide evidence they may or may not have complied with compliance policies and procedures and established internal control requirements.

Finally, you should keep track of external and internal events which may cause change 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, i.e., a company reorganization or major acquisition. This is also true of ongoing risk assessments. The 2012 Anti-Bribery & Corruption Guidance specified, “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, effective compliance programs, meaning those that do not simply exist on paper, but are operationalized, 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.” This same concept is brought forward into this prong of the 2019 ABC Guidance.

**Culture of compliance** – How often and how does the company measure its culture of compliance? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management’s commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

Culture in this context refers to not only the compliance policies and procedures in place, but knowledge and beliefs of those who abide by them which are formulated through observation of the organization’s activities. The compliance culture, or lack thereof, permeates through the organizational environment and influences the behavior of employees including middle and senior management. While the oversight of this concept ultimately falls in the hands of the board of directors, senior and middle management offer imperative perspective on how it's working in the day to day. This may be more difficult to measure as it is an intangible concept, but input can be derived from surveys or discussions with employees. Ongoing discussion of compliance, changes to policies and procedures, or general “town-halls” help infuse the compliance culture into the organization. This is far more beneficial than to have policies and procedures exist as an ornament in an otherwise dysfunctional compliance environment.

**B. Investigation of misconduct**

The next area the 2019 ABC Guidance addresses is investigations as a key element of an effective compliance program, which “is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company’s response, including any disciplinary or remediation measures taken.” It includes the following queries:

**Properly scoped investigation by qualified personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

Your company should have a detailed written procedure for handling any complaint or allegation of bribery or corruption, regardless of the means through which it is communicated. The mechanism could include the internal company hotline, anonymous tips, or a report directly from the business unit involved. You can make the decision on whether or not to investigate while consulting with other groups such as the Compliance Committee of the Board of Directors, or the Legal Department. The head of the business unit in which the claim arose may also be notified that an allegation has been made, and that the Compliance Department will be handling the matter on a going-forward basis. Through the use of such a detailed written procedure, you can work to ensure there is complete transparency on the rights and obligations of all parties once an allegation is made. This allows compliance to have not only the flexibility but also the responsibility to deal with such matters, from which it can best assess and then decide on how to manage the matter.

While this investigation protocol is critical to ensure each investigation is appropriately conducted and properly documented, each investigation will require the correct scoping. It should be adequately and accurately triaged. This leads to the need for independent and objective counsel. There are three reasons for a company to retain independent counsel for internal investigations of serious complaints. First, perception is reality, which means that for any corporate ethics and compliance program to be effective, it must be perceived to be fair. Second, if regular outside counsel investigates their own prior legal work or legal advice, a very large and potentially messy number of loyalty and privilege issues can arise in the internal investigation. The third reason relates to the relationship of the regular outside counsel or law firm with regulatory authorities. If a company's regular outside counsel performs the internal investigation and the results turn out favorably for the company, the regulators may ask if the investigation was a whitewash or at the very least, less than robust. If the SEC or DOJ cannot rely on a company's own internal
investigation, it may perform the investigation all over again with its own personnel.

**Response to investigations** – Have the company’s investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

Obviously, the investigation will be critical for you to help understand what remediation your compliance program will need. As Russ Berland, former CCO at Demantic Inc. has said, “Somebody found a way to get around your system. Maybe they colluded to overcome the internal controls. Maybe there was a group that simply wasn’t well-trained, didn’t understand, or there was a group that was extremely well-trained and decided to do it anyway. But somehow, there are issues in your system, and by system, the overall system of the executive tone, the governance, the compliance program, the internal controls, all at a meta level.”

It is axiomatic that you cannot finds gaps in your compliance system until you stress test it. Viewed in this light, your compliance failures can be viewed as such a stress test. Berland said, “You just got handed a stress test, and this is where the system broke down. Now you know there is a gap. Absent the investigation, as painful and difficult as that is, that gap would have just been sitting there.” The investigation will raise information to you about the failures of your compliance program that you may not have known existed previously.

While there will be a desire by some to not give out any information about the investigation until it is completed and there is a final report, you must resist this at all costs. If the results of the investigation are not made available to you as the CCO or the compliance professional charged with remediating the compliance program, any such remediation will be extremely difficult, because, as Berland noted, “you’re just going off suppositions and guesses.”

### C. Analysis and remediation of any underlying misconduct

The final area considered in the 2019 ABC Guidance focuses on reviewing the findings of what went wrong and fixing the problem going forward. This is also known as the remediation prong of a compliance regime. The 2019 ABC Guidance stated, “Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.” What are the lessons learned and more importantly, how did you put those lessons to use in the remediation of your compliance program going forward? This is more than simply the internal investigation, but a full root cause analysis of the issue which led to the breakdown. From there, the company must accept responsibility and take steps to remediate the failure, and to identify and prevent future risk.

**Root cause analysis** – What is the company’s root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

Here the DOJ is asking if you have performed a root cause analysis, how the analysis was designed and how the information from the analysis was used. The root cause analysis seeks answers to questions regarding the approval

"Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes."

2019 ABC Guidance
of activities prior to the occurrence of the event, the impact of the event, reasons for the system failure, be it interpersonal or systematic, and measures that could be implemented to prevent a reoccurrence. The root cause analysis is a value-added solution to gaps in your compliance program.

The key is that after you have identified the causes of problems, consider the solutions that can be implemented by developing a logical approach, using data that already exists in the organization. Identify current and future needs for organizational improvement. Your solution should be a repeatable, step-by-step process, in which one process can confirm the results of another. Focusing on the corrective measures of root causes is more effective than simply treating the symptoms of a problem or event and you will have a much more robust solution in place. This is because the solution(s) are more effective when accomplished through a systematic process with conclusions backed up by evidence.³

When you step back and consider what the DOJ was trying to accomplish with its 2019 ABC Guidance, it becomes clear what they expect from the compliance professional. Consider the structure of your compliance program and how it inter-relates to your company’s risk profile. When you have a compliance failure, use the root cause analysis to think about how each of the structural elements of your compliance program could impact how you manage and deal with that risk.

Prior weaknesses – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

What was the reason for the control failure? Was the control over-ridden by senior management? That was certainly one of the areas in the Panasonic Avionics FCPA enforcement action, where the CEO had his own designated slush fund that he had full control over with no oversight. A weakness could also come in the form of a control deficiency. For example, if the same person is able to approve and onboard a vendor, then later contract with the vendor and approve fraudulent invoices. When these control weaknesses are exposed, did you input a compensating control? If the violation occurred from a lack of control, did you review the system and implement a control or series of controls to prevent similar occurrences?

A company must show that it enforces compliance accountability through its compliance structures, authorities and responsibilities. A company must establish appropriate compliance performance metrics, for its compliance controls and, finally, clearly reward such persons through the promotion process in an organization. Such reward is through an evaluation of appropriate compliance measures and incentives. Interestingly a company must consider pressures that it sends through off-messaging. Finally, each employee must be evaluated in his or her compliance performance; coupled with both rewards and discipline for employee actions around compliance. You must have evidence that can demonstrate to an auditor there are processes in place to hold employees accountable for compliance breakdowns or failures.⁴

Payment systems – How was the misconduct in question funded (e.g., purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

Payroll controls and payment systems are a critical component of a best practices anti-corruption compliance program. This is because the design of an organization’s payroll controls must take into account the operational realities and risks attendant to the company’s business. There are several specific payroll controls which will facilitate operationalizing a compliance program. These controls help keep an eye on the money trail as the money to pay a bribe is usually hidden in some company expenditure. The four general areas of payroll control should include: (1) segregation of duties; (2) accountability, authorization, and approval; (3) security of assets; and (4) review and reconciliation.⁵

Vendor management – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

Third-parties are still the major source of compliance violations. Your vendor risk management program must take that level of risk into account. Yet here the 2019 ABC Guidance focuses precisely on that vendor risk management process. Do your vendors all go through the same third-party risk management process? Does it contain the following five steps: (1) business justification, (2) questionnaire, (3) due diligence and its
evaluation, (4) compliance terms and conditions, and (5) management by the business sponsor after the contract is signed? If this full process is not followed, what was the business reason for the granting of the exception? If no questionnaire was completed, was there an additional level of due diligence? What steps did you take to manage the relationship after the contact was signed? Have you ever audited any third parties? If not, what is your excuse? The questions posed by the DOJ make clear their intention to continue to emphasize compliance processes. The failure to establish or follow process will continue to get companies in hot water.

Prior indications – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company’s analysis of why such opportunities were missed? A root cause analysis is a method of dissecting your business process in order to review what went wrong so that the systems and processes can be remediated. The process will continue operating systematically as designed until change intervenes. Identifying blame does not necessarily help, rather root causes need to be identified, examined and remediated. The reason it is monikered “root cause analysis” is to emphasize the need to drill down below the superficial pieces of the framework to correct the areas that are actually driving the outcomes and the behaviors. In other words, you must treat the problem, not the symptoms. This leads to this series of questions about prior indications. A root cause analysis will give you insights into what happened by why it happened. This will provide the

DOJ information on the state of your compliance program at the time of the incident, which is one of its analysis under the FCPA Corporate Enforcement Program. The missed opportunity could have been because your hotline triage protocol did not accurately assess that whistleblower tip, or because a middle manager did not know what to do when one of their team members came into report something suspicious. It could have also been something much more serious such as a control weakness, outright failure, or fraud.

Remediation – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

When root cause analysis is done correctly and utilized as a part of your remediation strategy going forward, it is primarily there to develop preventive actions. A preventive action is something to prevent recurrence of the problem. You can adjust with a corrective action, but the ultimate goal is to engineer out or fix the system and processes so you do not have the opportunity for that flaw to occur again.6

In other words, it comes down to execution. This means you must use the risk management tools available to you and when a situation arises, you remediate when required. This is not only where the rubber hits the road, but the information and data you garner in the execution phase should be fed back into the process loop. From this, you will develop continuous feedback and continuous improvement.

Accountability – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company’s record (e.g., number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

The 2019 ABC Guidance ends with a series of questions around accountability. It begins at the micro level with questions on accountability specific to the incident(s) in question, and then moves to the macro-level about the company’s overall record on discipline. These questions emphasize a consistent theme of compliance programs which is document, document, document all of your actions. For if you do not do so, there may well be no information to present when the regulators come knocking.

One paramount area in the administration of discipline after any compliance related incident is consistency. Discipline must not only be administered fairly but it must be administered uniformly across the company for the violation of any compliance policy. If you are going to fire employees in South America for lying on their expense reports, you have to fire them in North America for the same offense. It cannot matter that the North American employee is a friend or a so-called “high producer.” Failure to administer discipline uniformly will destroy any vestige of credibility that you may have developed.7
IV. Conclusion

The 2019 ABC Guidance is yet another welcomed set of information from the DOJ. Further, it continues the DOJ’s (and SEC’s) steady emphasis on transparency and accountability which formally began with the 2012 FCPA Resource Guidance. In that 2012 offering, the DOJ and SEC first formulated the 10 Hallmarks of an Effective Compliance Program. Since that time, there has been continued communications from the DOJ on its views of a best practices compliance program. The 2016 FCPA Pilot Program, the 2017 Evaluation, and the 2017 FCPA Corporate Enforcement Policy all provided significant information on the state of compliance programs and insight into DOJ thinking when it reviews companies under a FCPA investigation.

Through this continued level of engagement, the DOJ is providing every CCO, every compliance practitioner, and every corporate compliance department with a clear and specific road map on how to design, create, implement and enhance a compliance program. The information is available and clear. By following these compliance best practices, you will create the chance for a better legal defense if you find yourself in an enforcement action. Yet more importantly, you will help make your company run more efficiently and more profitably.

A. Welcome to the OFAC compliance framework

In June, the Department of Treasury, Office of Foreign Asset Control’s (OFAC) released the Framework for OFAC Compliance Commitments (OFAC Framework). It is guidance for those entities seeking to comply with sanctions through a sanctions compliance program (SCP). Mike Volkov, one not normally associated with hyperbole, has called this “a game-changer.” I will be reviewing the OFAC Framework and exploring how it informs the ABC compliance practitioner.

OFAC itself said the OFAC Framework “strongly encourages” companies subject to its jurisdiction to take a “risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP).” OFAC recognizes that all businesses are different in “size and sophistication, products and services, customers and counter-parties, and geographic locations.” To this end each compliance program should not be a cookie cutter, off the shelf solution.

OFAC related that each corporate compliance program should be predicated on and incorporate at least five essential components of compliance:

1. Management commitment
2. Risk assessment
3. Internal controls
4. Testing and auditing
5. Training

However, OFAC stated that it would consider the robustness and implementation of these five prongs after conducting an investigation and in consideration of a civil penalty. Equally important, OFAC’s Office of Compliance and Enforcement (OCE) will also make a determination as to any of the five elements that should be incorporated into a corporate compliance program going forward as a part of any formal settlement agreement. The OFAC Framework goes on to state, “OFAC will evaluate a subject person’s SCP in a manner consistent with the Economic Sanctions Enforcement Guidelines (the “Guidelines”).”

Moreover, as OFAC applies the OFAC Framework to each specific fact pattern, it will favorably consider companies that have an effective compliance program. The OFAC Framework listed the following example, “under General Factor E (compliance program), OFAC may consider the existence, nature, and adequacy of an SCP, and when appropriate, may mitigate a CMP on that basis.” OFAC reiterated that its analysis is based on the five essential components of compliance listed above. Additionally, a company “may also benefit from further mitigation of a CMP pursuant to General Factor F (remedial response) when the SCP results in remedial steps being taken.”

With the increased sanctions program, most notably against Cuba, Iran and Venezuela, OFAC has demonstrated an aggressive policy of enforcement this year in particular.
In this new era of forceful OFAC sanctions enforcement, companies subject to OFAC jurisdiction need to be aware of the requirements for an effective SCP. As Volkov noted, “Companies that are in the process of implementing or updating their OFAC sanctions compliance program should review these documents and should incorporate these compliance expectations and elements into their own analysis.”

Finally, OFAC will most likely consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed “egregious.” The OFAC Framework provides companies with a structure for OFAC’s belief of the five essential components of a risk-based SCP. If a company under OFAC investigation has an “effective SCP” at the time of the violation, or if the subject implements remedial compliance measures at the time of the resolution, OFAC may reduce a penalty and/or deem the penalty non-egregious. This is what every compliance practitioner and compliance program needs to hear.

**Element 1 – Management commitment**

Under Management Commitment, a company must ensure that senior management demonstrates its commitment to, and support of, the organization’s SCP. This commitment is critical to ensure that the compliance program receives “adequate resources and is fully integrated into the day-to-day operations,” and helps “legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.” Effective management support includes the provision of adequate resources to the compliance unit(s) and support for compliance personnel’s authority within an organization. The term “senior management” itself is expansive including “senior leadership, executives, and/or the board of directors.”

To meet this requirement, there are five specific elements:

1. Senior management has reviewed and approved the organization’s compliance program. This means that the overall SCP should be reviewed, discussed and approved at the highest level of an organization. You should also be prepared to document those steps so be sure there are Board meeting minutes and other notations that all levels of senior management has actually performed this review and approval.

2. Senior management ensures that its compliance unit(s) have been delegated sufficient authority and autonomy to deploy the policies and procedures in a manner that effectively controls its OFAC risks. Senior management has to ensure the existence of direct reporting lines between compliance program functions and senior management, including routine and periodic meetings between these two elements of the organization.

This element requires two considerations. First, does the CCO, or whoever heads up the SCP, have access to senior management about the status of the company’s sanctions compliance risk management program? More than simply access, are there actual meetings where there is substantive discussion on issues around the SCP? This means more than simply quarterly, semi-annually or annually making a 15-minute presentation to the Board of Directors. Further, the prong of this element requires senior management to sit up and pay attention to trade sanction risk management.

3. Senior management has taken and will continue to take steps to ensure that the compliance unit(s) receive adequate resources – including in the form of human capital, expertise, information technology and other resources, as appropriate – that are relative to the organization’s breadth of operations, target and secondary markets, and other factors affect its overall risk profile. Under this element, OFAC outlined the following criteria: (a) The organization has appointed a dedicated OFAC sanctions compliance officer (who can also be responsible for other compliance programs); (b) The quality and experience of the compliance program personnel, including their technical knowledge and expertise, the ability of the personnel to understand complex financial and commercial activities, apply their OFAC knowledge, and identify OFAC-related issues, risks and prohibited activities; (c) The efforts to ensure that personnel dedicated to the compliance program have sufficient experience and appropriate “position” within the organization; and (d) Sufficient control functions exist to support the SCP, including but not limited to information technology software and systems. This prong has multiple elements as well. First, does
the person in charge of trade sanctions have real knowledge in the area or are those resources available to them? This is more than simply technical expertise, which is now simply table stakes. Do your trade compliance resource(s) understand the business well enough to understand both the trade compliance and business side? Put another way, can they read a spreadsheet in addition to understanding OFAC regulations. Next, are there sufficient resources put into a company’s trade sanctions risk management program, both from a budgetary perspective and a head count perspective? Finally, do you have an appropriate level of technological solutions delivered to and for the trade sanctions compliance program? If you are still using spreadsheets, you probably do not meet this requirement.

4. Senior management promotes a “culture of compliance” through the organization. Under this element, OFAC outlined the following criterial: (a) The ability of personnel to report sanctions related misconduct by the organization or its personnel to senior management without fear of reprisal; (b) Senior management messages and takes actions that discourage misconduct and prohibited activities, and highlight the potential repercussions of non-compliance with OFAC sanctions; and (c) The ability of the compliance program to have oversight over the actions of the entire organization, including but not limited to senior management, for the purposes of compliance with OFAC sanctions.

Both the DOJ Criminal Division’s Evaluation of Corporate Compliance Programs, 2019 ABC Guidance, and the Antitrust Division’s Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations focused on corporate culture as a key element of any best practices compliance program in their respective disciplines. It is therefore no surprise to see OFAC focus on it also, since it is now well-recognized of the need for a culture respecting and doing compliance in every organization. This prong requires senior management to fully embrace and support an internal reporting system for trade compliance issues and makes clear the repercussions for the failure to comply with a corporate trade SCP. Finally, does your trade SCP apply equally to everyone in the organization, literally from the shop floor up to the Boardroom?

5. Senior management demonstrates recognition of the seriousness of apparent violations of the laws and regulations administered by OFAC, or malfunctions, deficiencies, or failures by the organization and its personnel to comply with the SCP’s policies and procedures and implements necessary measures to reduce the occurrence of apparent violations in the future. Such measures should address the root causes of past violations and represent systemic solutions whenever possible.

This final prong of Element 1, demonstrates that OFAC has moved aggressively to remediate any trade sanction program violation, including discipling those involved. But more than simply personnel disciplines, OFAC mandates a root cause analysis (RCA) to understand the structural failures which may have led to, caused or allowed the violation(s) to occur. And finally, did senior management take what was learned in the RCA and use it to remediate the system?

Element 2 - Risk assessment

Every compliance professional of any stripe needs to read, understand and implement some of the key concepts of the OFAC Framework into your corporate compliance program. It does not matter if its trade controls, anti-corruption or anti-money laundering (AML). This OFAC Framework has much to offer that you should consider.

In any compliance regime, the starting point is a risk assessment. That is no different and certainly no surprise in the OFAC Framework. OFAC itself “recommends that organizations conduct a routine and ongoing risk assessment to inform its compliance program policies, procedures, internal controls and training.” In this respect, OFAC explained that such a risk assessment should consist of a “holistic review of the organization from top-to-bottom and asses its touchpoints to the outside world.”

Further, as you would expect, the OFAC Framework has a slightly different focus on risk than that articulated in Hallmark IV of the Ten Hallmarks of an Effective Compliance Program as initially formulated in the 2012 FCPA Resource Guide. Under the OFAC Framework, your compliance regime should assess the five following prongs: “(i) customers, supply chain, intermediaries, and counter-parties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks or systems; (iii) the geographic locations of the organization,
as well as its customers, supply chain, intermediaries and counter-parties; and (iv) potential merger and acquisitions, especially those involving non-U.S. companies or corporations.”

Under Prong 1, you need to consider not so much how you do business but with whom you do business. This is a slightly different focus on risk than under a Foreign Corrupt Practices Act (FCPA) risk assessment where the question is usually more focused on the use of third-party agents, distributors or others to sell to foreign officials or state-owned enterprises (SOEs). Yet the OFAC Framework focus is one that every compliance practitioner should consider as many bribery schemes now actively involve the customers and companies which enter into a relationship with your company through the supply chain.

Under Prong 2, you need to take a much more holistic view of your products and services than you would under a FCPA compliance program risk assessment. It is far beyond selling to foreign governments or SOEs. This Prong mandates you assess what you sell, where you sell it and how you sell it. However, from an overall business impact, this is certainly a much more business impactful manner to assess risk.

Prong 3 asks you to once again consider your “customers, supply chain, intermediaries and counter-parties” but this time from their home domicile or where they are providing goods or services to you. In this era of increasing transparency around extractive and other minerals, knowing where your products and services derive has moved from a nice piece of information to a mandatory inquiry.

Finally, under Prong 4, you should risk assess all merger and acquisition (M&A) candidates. Not only should you look at them from the ethics and compliance perspective but also from the trade sanctions perspective. Obviously, non-US companies will probably not have followed US export control or trade sanctions laws so you will need to be prepared to remediate as quickly as possible.

The next step is that an entity conducts, or will conduct, an OFAC risk assessment in a manner and with a frequency that adequately accounts for the potential risks. You should update your risk assessment to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business. In addition to the M&A component, there should be a similar exercise for third parties. The OFAC Framework noted, “On-boarding: The organization develops a sanctions risk rating for customers, customer groups, or account relationships, as appropriate, by leveraging information provided by the customer [for example, through a Know Your Customer or Customer Due Diligence process] and independent research conducted by the organization at the initiation of the customer relationship. This information will guide the timing and scope of future due diligence efforts.” This means you should develop a protocol for the risk rating of customers, vendors, or other relationships based on the due diligence process and independent research conducted by the organization at the initiation of the relationship. This information will guide the timing and scope of future due diligence efforts.

Finally, each organization should develop a “methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.” In other words, you cannot sit or stand still. Just as your business is ever evolving your OFAC Framework risk assessment should evolve to meet business opportunities and challenges.10
Element 3 - Internal controls

Not surprisingly, under the OFAC Framework, it is necessary that an effective compliance program have internal controls, including policies and procedures, to prevent, detect, escalate and report compliance related activity. OFAC also specifies that a key reason for this is to document these actions in any compliance framework. Internal controls are designed to define procedures and processes, such as those related to trade sanction compliance, and minimize the risks identified in your risk assessments.

The OFAC Framework recognizes the dynamic nature of compliance programs. It mandates that “policies and procedures should be enforced, weaknesses should be identified and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis.” In other words, your compliance program should have the ability to adjust rapidly to changes.

Under the OFAC Framework, Internal controls are systematic measures, such as reviews, checks and balances, methods and procedures, instituted by an organization that performs several different functions. These functions include allowing a company to conduct its business in an orderly and efficient manner; to assist an organization ensure the accuracy and completeness of its trade sanction information and data; to enable a business to produce reliable and timely management information; and to help an entity ensure there is adherence to its policies and procedures by its employees, applicable third parties and others. They should be entity wide. For compliance purposes, controls are measures specifically to provide reasonable assurance that any assets or resources of a company are not sold to any prohibited party or shipped out to a designated country.

To implement effective internal controls, the OFAC Framework lays out seven prongs which should be met. They include:

1. Written policies and procedure. Design and implement written policies and procedures outlining the compliance program. These policies and procedures should be relevant to the organization, capture your organization’s day-to-day operations, are written in the appropriate languages for the applicable business units, and not overly complex, such as overusing legal jargon. It is interesting to see OFAC view policies and procedures as internal controls. This is analogous to the Securities and Exchange Commission's (SEC) view that a Code of Conduct is an internal control as it pertained to its enforcement action involving United Airlines and its former Chief Executive Officer (CEO), Jeff Smisek.

2. Controls follow your risk assessment. Implement internal controls which sufficiently address the results of your organization's risk assessment. In other words, your internal controls should enable, prevent, detect, escalate and report compliance program activity. It also requires calibration of the controls “in a manner that is appropriate to address its risk profile and compliance needs. It is incumbent to consider not only the most obvious risk areas for your internal controls, but also the universe of potential transactions within the operations of a company. There is a clear need for rigor in your internal controls protocols and adherence to that rigor can increase operationalization around the internal controls a company should consider including gifts, travel and entertainment expenses. Finally, you should routinely test your controls to ensure design and operating effectiveness.

3. Testing of your controls. Effectiveness and adherence to your policies and procedures should be tested through both internal and external audits. This process should allow you to compare the internal controls actual performance to expected performance in order to determine whether it is meeting
its objectives and using resources effectively. Moreover, it is a technique that businesses use to determine what steps need to be taken to move from their current state to their desired future state.

4. **Document, document, and document.** Ensure that you document your policy, both design and retention, and adequately document your compliance program activities. You need to report your findings with the appropriate data and analysis presented, showing the strategic objectives, current standing, deficiencies, and whether the current situation is acceptable. Finally, all your analysis will be backed up with the data gathered during the analysis.

5. **Root cause analysis.** When you learn of a complete lack of certain controls, or the existence of, a control weakness, relating to trade compliance, take immediate and effective action, to the extent possible, to identify and implement controls until the root cause of the weakness can be determined and remediated. If the situation is unacceptable, you should present a course of action for improvement.

6. **Communicate.** You should clearly communicate your policies and procedures to all relevant staff, including compliance personnel, process owners and business units operating in high-risk areas and to external parties performing compliance program responsibilities on behalf of your organization.

7. **Responsible personnel.** You must have personnel to integrate these policies and procedures into the operations of the organization.

This includes relevant business units and you must work to make sure that the employees in any high-risk areas understand your organization's policies and procedures.

The internal control requirement under the OFAC Framework is not something new to the compliance practitioner. However, the seven prongs OFAC has laid out is a good way to think through the design, creation and implementation of your internal controls around trade sanctions.

### Element 4 - Testing and auditing

OFAC requires companies to assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. A comprehensive and objective testing, or audit program, of the compliance program ensures that a company has identified program weaknesses and deficiencies and it is the company's responsibility to enhance its program, including all program-related software, systems, and other technology, to remediate any identified gaps. Such enhancements might include updating, improving, or recalibrating compliance program elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of the compliance program or at the enterprise-wide level.

Under this element, a company has to implement three specific prongs:

1. A company ensures that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization. There are three general requirements under this prong. First, both the testing and audit functions for trade control must have a line of sight into senior management. Second, the testing and audit function is separate from design and application of the trade control functions (akin to auditor independence). Finally, the testing and audit functions must not only have authority to do their job but they must be capable of doing so; both from an ability and staffing view.

2. A company employs testing or audit procedures appropriate to the level and sophistication of its compliance group and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls. The key under this prong is "comprehensive and objective." Your audit team must be able to do a robust and thorough audit of your trade compliance program. Further, it must be truly objective.

3. A company ensures that upon learning of a confirmed negative testing result or audit finding pertaining to its compliance program, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated. If you find a deficiency or gap, you must move forward to remedy it. But more than simply implementing a remedy, you perform a root cause analysis to understand the true cause of any failure.
Element 5 - Training

Under the Training element, a company must, at a minimum, annually conduct training for relevant employees and personnel. To meet this requirement, a company must satisfy five basic criteria:

1. A company must ensure that its OFAC-related training program provides adequate information and instruction to employees and other stakeholders, such as clients, suppliers, business partners, and counterparties. Such training should be further tailored to high-risk employees within the organization. This prong presents two requirements: (1) effective training and (2) tailored training. Obviously, high-risk employees should participate in trainings that pertain to high-risk processes and activities. But you need to find a way to ensure, and then document, that you have provided training that actually informs on not only trade compliance risks, but the requirements of your trade compliance program. Finally, what training, if any, have you considered or put on for other stakeholders?

2. A company commits to provide OFAC-related training with a scope that is appropriate for the products and services it offers for customers, clients, and partner relationships it maintains in the geographic regions in which it operates. This requirement suggests that there must be a robust risk management system in place to continually assess the ever-changing trade sanctions risks for your company's business model. Certainly, the US trade sanction policy is foremost and paramount, but you should be cognizant of other countries as well. Moreover, you must have your finger on the pulse of the business to know and understand what risks are changing in your organization.

3. A company commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile. Obviously, this will vary from company to company and even position to position. However, in this now daily landscape of changing trade sanctions by the current administration, there clearly needs to be both ongoing internal dialogue and internal training to fit the current political circumstances.

4. A company must ensure that when it becomes aware of a confirmed negative testing result, audit finding, or other deficiency pertaining to its compliance program, it will take immediate and effective action to provide training to or other corrective action with respect to relevant personnel. This makes clear not only the need for testing but also follow up on that testing to determine if the students actually passed or if they might have some deficiency which needs to be remediated.

5. A company’s training program includes easily accessible resources and materials that are available to all applicable personnel. This means that the materials should be written in a direct and understandable manner, and not overly use legal jargon. It also means you must translate the training materials into the native language of your employee base. This is true even if your company has an English-only policy for corporate communications, all your training materials need to be available and accessible in local languages.

There is quite a bit in this OFAC Framework for the anti-trust/anti-bribery compliance practitioner. While the OFAC Framework has a different focus, it can provide the anti-trust/anti-bribery compliance practitioner with helpful information about not only what the DOJ is thinking when it comes to its expectations of a compliance program, but also benchmarks for best practices.
V. The Antitrust division guidance on an effective compliance program

As the third in a triumvirate of releases on compliance programs, the DOJ Antitrust Division, in July, released its Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (Antitrust compliance program guidance). Following the releases of the DOJ Criminal Division’s 2019 ABC Guidance in April and the Office of Foreign Asset Control OFAC Framework in May. These three documents go a long way in cementing the need for robust and effective compliance for corporations.

A. Introduction

The Antitrust compliance program guidance significantly changes the calculus by the government when prosecuting a criminal antitrust violation. Regarding the Leniency Program, Mike Volkov of the Volkov Law Group noted, “Since the 1990s, the Antitrust Division’s policy regarding corporate compliance programs was generally fixed given the ability of companies to seek benefits under the leniency program. In this respect, the first reporting company would earn immunity and a de-trebling of civil liability for antitrust cartel conduct.” However, if your organization was not the first to self-report, you could not avoid a criminal penalty for violation of antitrust laws. It was purely a race to see which organization could first self-report to the DOJ.

This has changed under the Antitrust compliance program guidance as it incentivizes companies to create effective Antitrust compliance program guidance by creating credit which the government may allot at the charging stage of an antitrust violation. This means that the Leniency Policy created in the 1990s for the first to self-report has now been expanded so that a company which no longer is the first to report can receive up to a Declination if certain criteria are met. Put another way, good corporate citizens who are not the first but do self-report, thoroughly investigate the violation, extensively cooperate with the government and have an effective compliance program under the Antitrust compliance program guidance can receive a significant discount up to a Deferred Prosecution Agreement (DPA) for criminal antitrust violations.

The purpose of the Antitrust compliance program guidance is threefold. The purposes, authored by the Antitrust Division, include a manner to credit compliance programs at the charging stage of an antitrust indictment; clarifying the Antitrust Division’s approach to evaluating effectiveness of compliance programs at the charging stage; and, finally, to provide a public guidance document for the evaluation of compliance programs, once again from the antitrust perspective. In addition to these three considerations made at the charging stage, the Antitrust compliance program may also come into play at any sentencing stage. Mr. Volkov stated, “Under the existing Sentencing Guidelines, a company can earn a three-point reduction in its culpability score if the company has an “effective” compliance program. Second, a compliance program may be
relevant to determining the appropriate corporate fine to recommend within the guidelines range, or even below the range in extraordinary circumstances. And third, the existence of a compliance program is relevant to the government’s recommendation on probation.”

Jesse Caplan, Managing Director, Affiliated Monitor Inc. (AMI), noted in a podcast interview on the FCPA Compliance Report that this new Antitrust compliance program did not come “out of left field and I think that’s consistent with where the Department of Justice is going. Arguably it is the next step after the Leniency Program has been in place for quite a number of years.” He also believes that beyond simply assisting the Antitrust Division in prosecuting, the Antitrust compliance program provides “incentives to any other companies for truly making sure that they had a very effective antitrust compliance program, to ensure that they are good corporate citizens and that they have effective compliance programs.”

The Antitrust compliance program guidance itself states that it focuses on the “evaluation of compliance programs in the context of criminal violations of the Sherman Act such as price fixing, bid rigging, and market allocation. It is intended to assist Division prosecutors in their evaluation of antitrust compliance programs at the charging and sentencing phases of an investigation. Although the evaluation of antitrust compliance programs is an important factor in the prosecutorial decision-making process at both charging and sentencing, a number of other important factors not addressed by this compliance- specific guidance also must be considered.”

Moreover, “effective antitrust compliance programs not only prevent, detect, and address antitrust violations, they also further remedial efforts and help foster corporate and individual accountability by facilitating a corporation’s prompt self-reporting and timely and thorough cooperation in the Antitrust Division’s investigations. Indeed, a truly effective antitrust compliance program gives a company the best chance to obtain the significant benefits available under the Division's Corporate Leniency program.”

As you would expect from the DOJ, the Antitrust compliance program guidance will not be applied in a formulaic manner but with a more flexible approach. There are three “fundamental questions” prosecutors will have to consider in their evaluation. They are (1) Is the Antitrust compliance program well designed? (2) Is the Antitrust compliance program being applied earnestly and in good faith? And (3) Does the Antitrust compliance program work?

Once again emphasizing that these questions are not to be applied as a formula checklist, the Antitrust compliance program guidance goes on to lay out the factors of an effective program. The Antitrust compliance program guidance cautions, “Indeed, not all factors will be relevant in every case, and some factors in the Division’s analysis are relevant to more than one question. Moreover, the Division recognizes that a company’s size affects the resources allocated to antitrust compliance and the breadth of the company’s compliance program.” Prosecutors are cautioned that they “should evaluate compliance programs throughout the course of their investigation, including asking relevant compliance-related questions of witnesses, and should not wait for companies to offer a compliance presentation before beginning their evaluation of a company’s antitrust compliance program.”

B. Elements of an effective Antitrust compliance program

The next areas for consideration are the elements set forth by the Antitrust Division which constitute an effective compliance program. The Antitrust compliance program guidance notes that the goal of an effective compliance program is to “prevent and detect violations.” Further, while the DOJ states, “no compliance program can ever prevent all criminal activity by a corporation’s employees,” the “critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct.” The Antitrust compliance program goes on to state, “[t]he keys for successful [antitrust] compliance [programs] in general are efficiency, leadership, training, education, information and due diligence.”

To that end, the Antitrust compliance program guidance lists nine separate elements which should go into an effective antitrust compliance program. They will be familiar to every
compliance practitioner. These include (1) the design and comprehensiveness of the program; (2) the culture of compliance within the company; (3) responsibility for, and resources dedicated to, antitrust compliance; (4) antitrust risk assessment techniques; (5) compliance training and communication to employees; (6) monitoring and auditing techniques, including continued review, evaluation, and revision of the antitrust compliance program; (7) reporting mechanisms; (8) compliance incentives and discipline; and (9) remediation methods.

Under element no. 1, Design and Comprehensiveness, the DOJ will always see through a paper program, which by definition, will not be effective at any rate. Prosecutors are directed to consider the “design, format and comprehensiveness of an antitrust compliance program” as well as its “integration into the company’s business and accessibility to employees.” Questions posed by the Antitrust compliance program include the following:

- When was the program implemented? Updated? Reviewed, assessed, refreshed and upgraded?
- Is the program in writing?
- Who is responsible for the program? Is it integrated with and mapped to the company’s internal controls program?
- Has the company’s antitrust risks been assessed? How often has this been updated?
- Has the company put out guidance to employees on this policy? How about document destruction and obstruction of justice in relation to investigations?

The second element is the “Culture of Compliance” and here the DOJ states that an effective antitrust compliance program will “promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.” Recognizing that such support must flow down from the top of an organization, the support of an antitrust compliance program from the company’s top management is critical to success. Senior management must convince employees “of the corporation’s commitment to the compliance program.” Here prosecutors are required to consider the following questions.

- Has senior management not only talked the talk but also walked the walk of compliance? What concrete actions have they taken to do so? What has senior management done to change the company’s culture of compliance?
- Has senior management tolerated violations in the past or been involved in antitrust violations?
- Is there personal accountability at the senior management level?

The third element centers on the Chief Compliance Officer (CCO) and their autonomy, authority and seniority within your organizations overall corporate governance as well as resources in both headcount and monetary means to accomplish ongoing training, auditing and evaluation and assessment of your antitrust compliance program. Some of the questions posed for prosecutors include:

- Who is responsible for the antitrust compliance program? Do they report to the Board of Directors? How is the CCO ensured of independence? What is the stature, rank, compensation of the CCO and is the position senior within the organization?
- What is the structure of the corporate compliance function? Are they subject matter experts? Who do they report to and what is the format of that reporting?
- Are sufficient resources dedicated to the antitrust compliance function, both in terms of headcount and monetary funding? Who reviews the effectiveness of the compliance function?

The fourth element is risk assessments. As with all corporate compliance programs, it all begins with each organization assessing its own risks and then tailoring its compliance program to manage those risks. Under this element, some of the questions include:

- Is your organization’s antitrust compliance program tailored to the organization’s industries/business lines and consistent with industry best practice? For example, as employees utilize new methods of electronic communication, what is the company doing to evaluate and manage the antitrust risk associated with these new forms of communication?
- Is the company’s risk assessment subject to periodic review and update? Are new or enhanced risks incorporated into your antitrust compliance program risk management calculus?

Element no. 5 refers to training and communication. The Antitrust Division stated, “Ideally, [antitrust compliance training] empowers employees to do business confidently insofar as
they are clearer on what is and is not permissible and can resist pressures more effectively (whether these are internal or external)." Not only should training be risk based but it should also focus on educating employees on how and when legitimate business collaboration becomes “problematic” and may result in illegal conduct. Some of the questions posed for prosecutors include:

- How has the company communicated its antitrust policies and procedures to all employees and in an effective manner which promotes understanding? In what specific ways are antitrust compliance policies and procedures reinforced through the company’s internal controls?
- It is not enough to simply translate antitrust policies, procedures and training into local languages but any barriers to effective understanding must be addressed. How has the company addressed these barriers?
- Are there mechanisms to track the effectiveness of training and ensure that it is being followed? Is there certification of training and sign-off of policies and procedures?
- What is the basis for who receives the training? Is it risk-based in terms of time and business opportunity? How often is the training updated?

The sixth element is periodic review, monitoring and auditing. The Antitrust Division stated an organization should, “Periodically assess whether parts of [a] company’s business or certain business practices are complying with antitrust laws in practice allows senior managers to know whether the company is moving closer to its antitrust compliance objectives.” Not only does such periodic testing help “ensure that there is continued, clear and unambiguous commitment to antitrust compliance from the top down” but also, if the antitrust risks have changed then there should be a reassessment of the risk mitigation activities and controls to ensure they remain appropriate and effective. Some of the questions under this element include:

- What method is used to evaluate your antitrust compliance program, how is it done and who does the evaluation?
- What ongoing monitoring and auditing mechanisms are used to prevent and detect antitrust violations?
- What is the company’s process for ongoing improvements to the antitrust compliance program?

The seventh element is reporting. This includes confidential reporting mechanisms as well as the promotion of a “speak up” culture. Some of the questions posed here include:

- Is the reporting system publicized internally? Can employees make anonymous reports? Is there whistleblower anti-retaliation protection?
- Are supervisors required to notify superiors if a potential violation is reported to them? Are there disciplinary measures in place for the failure to do so?
- Is there an investigation protocol in place if a potential violation is reported?

The eighth element is incentives and discipline, i.e. both the carrot and the stick, around your antitrust compliance program. Some of the questions posed include the following:

- What incentives are in place to promote the antitrust compliance program? What considerations have been given to theses incentives, compensation structure and rewards?
- Are disciplinary measures in place and have they actually been used? Has there been any management turnover based upon antitrust issues? Are the disciplinary measures consistent with other types of misconduct?
- For senior executives who may have been involved in improper behavior, did they cooperate with the investigation and have they accepted responsibility for their actions?

Finally, we have element nine regarding remediation of any violations and the role that the company’s antitrust violation played in the discovery of the violation. Obviously, the robustness of
both the investigation and remediation are critical elements in not only a compliance program but also in seeking credit under the US Sentencing Guidelines. However, using the compliance program to detect violations can also have the added benefit of allowing a company to be the first to report under the Leniency Program, which of course can lead to a full pass on any criminal charges. Some of the questions posed by prosecutors under this element include:

— What role did the antitrust compliance program play in uncovering the violation? If so how and was the violation reported up the chain?
— Was a root cause analysis performed? What remediation occurred as a result of the root cause analysis?
— What was the role of outside counsel in this process? What role did senior management play?
— Were policies and procedures updated based upon the remediation? Has any update been the subject of training and certification?
— Did the compliance program assist the company in promptly reporting the illegal conduct? Did the company report the antitrust violation to the government before learning of a government investigation? How long after becoming aware of the conduct did the company report it to the government?

While many of these queries will be familiar to the anticorruption/antibribery (ABC) compliance practitioner, there are some new twists that could be useful for those not in antitrust compliance to consider going forward. We will later consider differences of an ABC compliance program.

C. Sentencing considerations

How will all of this will be used in Sentencing Considerations? Interestingly, the Antitrust compliance program provides for sanction and penalty reduction at two different times during the investigative process; at the charging phase and at the sentencing phase. According to the Morrison & Foerster LLP newsletter, Quarterly Cartel Catch-Up: Recent Developments in Criminal Antitrust for Busy Corporate Counsel, July 2019, “at the charging stage, the guidance indicates that prosecutors will consider three preliminary questions: (1) whether the compliance program addresses and prohibits criminal antitrust violations; (2) whether the compliance program detected and facilitated the reporting of the violation; and (3) to what extent senior management was involved in the violation. The guidance then lists nine factors prosecutors should use to evaluate the effectiveness of the program.”
However, at the sentencing phase, the Antitrust compliance program guidance “details the three ways in which an effective compliance program can impact a corporate defendant’s sentence. First, an effective compliance program could lead to a three-point reduction of the corporation's culpability score under the U.S. Sentencing Guidelines. Second, an effective compliance program could lead prosecutors to recommend a below-Guidelines fine. Third, the effectiveness of a compliance program will factor into prosecutors’ recommendation for probation or an external corporate monitor.” During his speech announcing the Antitrust compliance program, Assistant Attorney General, Makan Delrahim, stated “that the Division had not yet recommended the three-point credit under the Guidelines but had advocated for a reduced fine when a company had taken great efforts to change its corporate culture after a violation.”

The three-point reductions are not available where there has been, according to the Antitrust compliance program, “an unreasonable delay in reporting the illegal conduct to the government.” Acknowledging that there is a presumption that antitrust compliance programs are not effective. To overcome this presumption, prosecutors are directed to make a five-step inquiry of the following issues: “(i) individuals with operational responsibility for the compliance program had direct reporting obligations to the governing authority of the company (e.g., an audit committee of the Board of Directors if applicable); (ii) the compliance program detected the antitrust violation before discovery outside of the company or before such discovery was reasonably likely; (iii) the company promptly reported the violation to the Antitrust Division; and, (iv) no individual with operational responsibility for the compliance program “participated in, condoned, or was willfully ignorant” of the antitrust violation.”

In criminal cases where the Antitrust Division is determining whether or not to recommend probation, a key inquiry is whether the culpable individuals have left the company. This is even if the company has accepted responsibility for its actions and fully cooperated with the DOJ. Finally, if a company did not have an antitrust compliance program in place at the time of the violation(s), all is not lost. If a company puts a compliance program in place, those actions can be evaluated. Moreover, “If the company has not established an adequate compliance program, the Division may recommend probation and, in appropriate cases, periodic compliance reports as a condition of probation. The Division also will consider whether an external monitor is necessary to ensure implementation of a compliance program and timely reports.”

Finally, the Antitrust compliance program guidance also has a mechanism for reducing the overall fine and penalty, stating, “In determining whether to impose a fine, and the amount and timing of that fine, courts shall consider any measure taken by a company to discipline personnel responsible for the offense and to prevent recurrence of the offense. Division prosecutors thus should consider whether a company’s extraordinary post-violation compliance efforts warrant a fine reduction.”

What must a company do to “warrant a fine reduction”? It begins with a “dedicated effort” to change the company's culture to one of compliance. The Antitrust compliance program guidance then lays out four other inquiries:

- **Tone at the Top** – What steps has senior management taken to require and incentivize lawful behavior and participation in compliance training? Has the company demonstrated that ensuring future compliance and culture change is paramount?
- **Improvements to Pre-Existing Compliance Program** – Has the company conducted a comprehensive review of its compliance, training, monitoring, auditing, and risk control functions following the antitrust violation? How did the
company modify and revise its compliance program to prevent similar conduct from reoccurring?

— Creation of Compliance Program – Did the company create a robust program tailored to the company’s business and aimed at preventing recurrence of an antitrust violation? Does the company’s new antitrust compliance program educate employees about the illegal conduct that occurred as well as other antitrust risks?

— Disciplinary Procedure – Did the company have or create disciplinary procedures for employees who violate the law or the company’s compliance program? Did the company discipline employees who engaged in the violation?

D. What does it mean for ABC compliance?

What does the Antitrust compliance program guidance means for the antitrust compliance professional and anticorruption/antibribery compliance (ABC) programs going forward? Recognizing that the Antitrust compliance program is designed to prevent, detect and then remediate illegal antitrust behavior, including anti-competitive and cartel actions, nevertheless, it is not only instructive for the ABC compliance professional.

In the area of Design and Comprehensiveness, the Antitrust compliance program asks such questions as “Who is responsible for integrating antitrust policies and procedures into the company’s business practices? In what specific ways are antitrust compliance policies and procedures reinforced through the company’s internal controls?” This leads directly into the next area of inquiry about tracking. This refers to tracking employee actions and conduct in high risk areas and at high risk events. The Antitrust compliance program inquiries into company’s actions around not only monitoring business contacts with competitors, but also attendance at trade shows, association meetings and if these systems are regularly monitored.

Also, if employees are required to or regularly attend such events, are they receiving not only training on appropriate (and illegal) conduct but are they receiving targeted reminders? All of these tactics should be embraced by the ABC compliance professional as a way to monitor data as specifically noted in the Antitrust compliance program such as pricing changes and bidding activity. Finally, with the growing number of FCPA enforcement actions where the customer itself is a part of the bribery scheme, this type of data and transaction monitoring is becoming even more critical.

While the ABC Guidance spoke to culture, the Antitrust compliance program guidance says, “employees should be ‘convinced of the corporation’s commitment to [the compliance program].’” Moreover, the Division will “examine the extent to which corporate management has clearly articulated — and conducted themselves in accordance with — the company’s commitment to good corporate citizenship.” This same concept, “being a good corporate citizen” should be incorporated into every ABC compliance program.

The Risk Assessment in the Antitrust compliance program guidance mandates review of a company’s “lines of business.” It poses the question not seen in the 2019 ABC Guidance “Is the company’s antitrust compliance program tailored to the company’s various industries/business lines and consistent with industry best practice?” That not only uses ‘business lines’ language but also “consistent with industry best practices.” This is something that should be taken to heart by every ABC compliance professional. If the DOJ’s FCPA Unit comes knocking, you will be in much better position if you have met both of these Antitrust compliance program guidance mandates.
Risk assessment also points to metrics not seen in the 2019 ABC Guidance. It asks, “What information or metrics has the company collected and used to help detect antitrust violations? For example, if the company bids on contracts, is bid information subject to evaluation to detect possible bid-rigging? Does the company evaluate pricing changes for possible price-fixing?” From the ABC perspective, you should consider if you are using both bid and final contract pricing to determine if bribery and corruption is occurring. The numbers are there for analysis. It would not take too long to see that the FCPA Unit will soon be asking to see your analysis of both bid prices and contract prices from the ABC perspective in addition to the antitrust perspective.

Under Training, both the Antitrust compliance program guidance and the ABC Guidance specify targeted and effective training. Yet the Antitrust compliance program guidance adds several components that every ABC compliance practitioner should well consider incorporating into their training. It asks, “How often is antitrust training updated to reflect marketplace, legal, technological, or other developments? Has the training addressed lessons learned from prior antitrust violations or compliance incidents?” The updating of training to reflect “marketplace, legal, technological or other developments” should be mandatory for the ABC compliance professional. For instance, have you incorporated regime change into your compliance training or that customers are now seen as a part of bribery scheme and incorporated the most recent enforcement actions where this occurred into your training?
It is in the area of Periodic Review, Monitoring and Auditing that a clear advance in data and data analytics is seen in the Antitrust compliance program. Here, the Antitrust Division expects a company to actively look for violations through detection and prevention. The Antitrust compliance program guidance states a company should engage in a “periodic review of documents/communications from specific employees; performance evaluations and employee self-assessments for specific employees; interviews of specific employees.” The well-worn excuse that if we look, we might find something is rightfully relegated to the dustbin of ostrich behavior.

But the Antitrust compliance program guidance mandates more than simply watching your employees. It states, “Does the company use any type of screen, communications monitoring tool, or statistical testing designed to identify potential antitrust violations?” Both the traditional approach of monitoring and interviewing coupled with a statistical analysis to see if there are any anomalies should be used by the ABC compliance professional to review information in their organization to determine if there are any indications of bribery & corruption violations.

The bottom line is that there is much for the ABC compliance practitioner to learn from the Antitrust compliance program guidance. The data analytics, transaction monitoring and statistical analysis are all tools which need to be incorporated into an ABC compliance program. Each of these tactics will improve not only your compliance program but make your business processes run more efficiently and at the end of the day, make your company more profitable.
VI. Conclusion

2019 was a very significant year for every compliance practitioner and compliance program. There were three significant releases of information by the federal government which directly impacted compliance professionals in 2019. Two came from the Department of Justice (DOJ) and one came from the Department of Treasury, Office of Foreign Asset Control (OFAC).

First, Assistant Attorney General Brian Benczkowski announced an update to the 2017 Evaluation of Corporate Compliance Programs, entitled Evaluation of Corporate Compliance Programs - Guidance Document (2019 Guidance). It is mandatory reading for every Chief Compliance Officer (CCO), compliance practitioner and professional or any other person interested in the latest thinking from the DOJ on what constitutes a best practices compliance program.

The 2019 Guidance posed three “fundamental questions” that prosecutors must begin their analysis with:

1. “Is the corporation’s compliance program well designed?”
2. “Is the program being applied earnestly and in good faith?” In other words, is the program being implemented effectively?
3. “Does the corporation’s compliance program work” in practice?
Next, OFAC released the Framework for OFAC Compliance Commitments (OFAC Framework). It provides guidance for entities seeking to comply with sanctions through a Sanctions Compliance Program (SCP). Mike Volkov, one not normally associated with hyperbole, has called this “a game-changer”.

The OFAC Framework “strongly encourages” companies subject to its jurisdiction to take a “risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP).” OFAC recognizes that all businesses are different in “size and sophistication, products and services, customers and counterparties, and geographic locations”. To this end each compliance program should not be a cookie cutter, off the shelf solution.

OFAC related that each corporate compliance program should be predicated on and incorporate at least five essential components of compliance:

1. **Management Commitment**
2. **Risk Assessment**
3. **Internal Controls**
4. **Testing and Auditing**
5. **Training**

The OFAC Framework had a key emphasis on vendors in the Supply Chain as well as customers mandated in ongoing due diligence.
Finally, in July, the DOJ Antitrust Division released its Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (Antitrust Guidance). Together with the 2019 Guidance and OFAC Framework, these three documents go a long way in cementing the need for robust and effective compliance for corporations.

The Antitrust Guidance significantly changes the calculus by the government when prosecuting a criminal antitrust violation. Regarding the Leniency Program, Volkov noted, “Since the 1990s, the Antitrust Division’s policy regarding corporate compliance programs was generally fixed given the ability of companies to seek benefits under the leniency program. In this respect, the first reporting company would earn immunity and a detrebling of civil liability for antitrust cartel conduct.” However, if your organization was not the first to self-report, you could not avoid a criminal penalty for violation of antitrust laws. It was purely a race to see which organization could self-report to the Antitrust Division first.

This has changed under the Antitrust Guidance as it incentivizes companies by creating credit which the government may give at the charging stage of an antitrust indictment. The Leniency Policy created in the 1990s for the first to self-report has now been expanded so that a company which no longer is the first to report can receive up to a Declination if certain criteria are met. Put another way, good corporate citizens who are not the first but do self-report, thoroughly investigate the violation, extensively cooperate with the government and have an effective compliance program under the Antitrust Guidance can receive a significant discount up to a Deferred Prosecution Agreement (DPA) for criminal antitrust violations.

The purpose of the Antitrust Guidance is threefold. First, it provides manner to credit compliance programs at the charging stage of an antitrust indictment. Second, it clarifies the Antitrust Division’s approach to evaluating effectiveness of compliance programs at the charging stage. Thirdly, it provides a public guidance document for the evaluation of compliance programs, once again from the antitrust perspective. In addition to these three considerations made at the charging stage, the Antitrust Guidance may also come into play at any sentencing stage. Volkov stated, “Under the existing Sentencing Guidelines, a company can earn a three-point reduction in its culpability score if the company has an “effective” compliance program. Second, a compliance program may be relevant to deter mining the appropriate corporate fine to recommend within the guidelines range, or even below the range in extraordinary circumstances. And third, the existence of a compliance program is relevant to the government’s recommendation on probation.”
Moving forward into 2020 and beyond, this may be the most significant message for every compliance practitioner and compliance program.

These three documents provided not only the government’s refreshed thinking on what constitutes a best practices compliance program but lays out specific, actionable items every compliance practitioner can take to implement them in a corporate compliance program. While each document focuses on areas specific to that discipline; anti-corruption compliance, anti-trust compliance and trade sanction compliance, taken together it drives home the message of the convergence of compliance from disparate disciplines together into one overall ‘compliance’ function.
Document sources:

About the author

Jonathan specializes in global and complex corporate investigations (White Collar Crime) and other investigations. He has 30+ years of experience working closely with clients, their board, audit committee, senior management, internal audit, compliance, legal and outside law firm on global/domestic fraud, misconduct, cyber incidents, bribery, money laundering, whistleblower and retaliation matters, and when appropriate conducting an investigation (10A, books and records, cross-border, FCPA, regulatory etc.), then determines economic damages, performs root cause analysis, develops remedial procedures, and designs/enhances governance, global risk management and compliance systems along with internal controls, policies and procedures and monitoring tactics to mitigate future potential issues. He also testifies when called upon.

Jonathan has deep expertise in accounting (GAAP), auditing (GAAS/PCAOB) and SEC matters. He has worked with companies, their auditors, management and regulators on highly-technical issues.

Jonathan is skilled in SEC reporting, registrations and compliance with the Securities Act of 1933, the Exchange Act of 1934, the False Claims Act (FCA) the Racketeer Influenced and Corrupt Organizations Act (RICO), the Foreign Corrupt Practices Act (FCPA), the Sarbanes-Oxley Act (SOx), California Notice of Security Breach Act, Dodd-Frank, and the UK’s Bribery Act (UKBA). He has been in the role of chief audit executive and compliance coordinator and built/enhanced internal audit and compliance programs, conducted financial, operational, and regulatory due diligence for mergers, acquisitions and 3rd parties.

He has educated and advised some of the world’s largest companies and organizations.

Jonathan also writes a blog that is focused on fraud, governance, risk and compliance. Visit his blog at www.boardandfraud.com.

Contributing author

Tom is literally the guy who wrote the book on compliance with his seminal one volume book “The Compliance Handbook” published in May 2018, which was the No. 1 new bestseller on Amazon.com through its initial run. Additionally, Tom has authored 16 books on business leadership, compliance, ethics and corporate governance, including the international best-sellers “Lessons Learned on Compliance and Ethics” and “Best Practices Under the FCPA and Bribery Act”, as well as his series Fox on Compliance.

Tom leads the social media discussion on compliance with his award-winning blog, The FCPA Compliance and Ethics Blog and is the Voice of Compliance, having founded the Compliance Podcast Network.