

## EXPERT ANALYSIS

### Justice Department Releases Standards for Evaluating Corporate Compliance Programs

By James Corsiglia, Esq.  
Cleary Gottlieb

The U.S. Department of Justice recently issued a statement, titled "Evaluation of Corporate Compliance Programs," that sets forth a series of questions on compliance- and remediation-related issues that the DOJ may probe when negotiating with companies accused of misconduct.<sup>1</sup>

How companies respond to those inquiries may impact whether the DOJ decides to bring charges, the nature of a corporate resolution (e.g., guilty plea, deferred prosecution agreement), and the size of any financial penalty.

As a result, any company facing a DOJ enforcement action will undoubtedly want to carefully review these questions before entering into settlement discussions with the Justice Department.

Regardless of whether companies are confronted with misconduct by their employees, it is likely that the compliance guidance will also frequently be used as a tool to review corporate compliance programs.

While the DOJ stresses that the compliance guidance is "neither a checklist nor a formula" for any particular company's compliance program, the guidance will nonetheless likely serve as a set of "best practices" against which companies can measure their compliance programs.

#### PUTTING THE GUIDANCE IN CONTEXT

The compliance guidance is not the first effort to shape compliance standards. Rather, governments, international organizations and non-governmental organizations have issued a seemingly endless parade of compliance advice. Most recently, the International Organization for Standardization issued the anti-corruption management system.<sup>2</sup>

The U.S. government has itself long engaged in a substantial effort to shape compliance programs for corporations that are subject to U.S. laws. An understanding of the development of U.S. compliance standards helps put the new guidance in context and gives a sense of where the DOJ may be headed as its views on compliance standards continue to evolve.

The guidance cites to five previous resources that compile the basis for many, but not all, of the compliance concerns it raises. Three of these resources come from the U.S. government, and two derive from international organizations.

First among the cited federal resources are the U.S. sentencing guidelines, which serve an advisory role when judges are determining criminal punishments.

The guidelines were amended in 2004 to provide for greater leniency if the company "had in place at the time of the offense an effective compliance and ethics program."<sup>3</sup> They identify the following components of an effective compliance program:

*The compliance guidance asks what the process was for designing the policies, who was involved and which business units were consulted.*

- A culture of ethical conduct.
- Diligence to prevent and detect criminal conduct.
- Policies and procedures.
- A board of directors that is adequately informed of the compliance program.
- Management responsibility for compliance.
- Specific individuals with day-to-day responsibility for compliance that have direct access to the board.
- A compliance function with independence, authority and adequate resources.
- Screening of management employees for a history of misconduct.
- Fair enforcement of compliance standards.
- Appropriate incentives and discipline for employees.
- Communication and training.
- Monitoring and auditing the program.
- Risk assessment.
- Modifying the program to respond to the risk assessment and compliance failures.

Years later, these elements largely comprise the framework for the new guidance.

The second source cited by the guidance — the manual governing the actions of federal prosecutors — generally directs federal prosecutors to use the sentencing guidelines' compliance standards when evaluating whether to bring charges against a company and in negotiating plea deals or other enforcement action settlements.<sup>4</sup>

The third U.S. government source cited in the guidance is the DOJ and the U.S. Securities and Exchange Commission 2012 guide to the U.S. Foreign Corrupt Practices Act.

This FCPA guide contains a section on compliance programs that essentially captures the standards set forth in the sentencing guidelines. It also provides additional guidance on mergers and acquisitions diligence and post-acquisition compliance integration, issues that are also covered in the new guidance.<sup>5</sup>

In its discussion of compliance programs, the FCPA guide also suggests substantive topics that companies should consider covering in anti-corruption policies, such as gifts, charitable donations and facilitation of payments.

The guidance also cites a brief "good practice" guide published by the Organization for Economic Co-operation and Development in 2010, which repeats many of the same components as the sentencing guidelines and an ethics handbook put out by the OECD, the U.N. and the World Bank in 2013.<sup>6</sup>

This handbook is a compilation of quotations from various other business ethics guides broken out into categories that, again, largely track the categories of a compliance program set forth in the sentencing guidelines (e.g., commitment from senior management, communication and training).

The handbook also proposes various techniques for conducting risk assessment and briefly mentions certain issues that might be covered by anti-corruption policies (e.g., conflicts of interest, extortion demands, payments of gifts and hospitality).

Thus, the new guidance should be viewed, in part, as another step in a long-standing DOJ compliance drive that has been largely shaped by the 2004 changes to the sentencing guidelines.

The sentencing guidelines' principal focus is on compliance administration and governance — ensuring that an appropriate structure is in place to identify issues, train personnel, assign management personnel and inform senior management and the board on compliance matters.

The FCPA guide supplements that focus on administration and governance by reference to the risks associated with M&A transactions and specific policies for high-risk corporate activities, such as giving gifts to or interacting with government officials.

While embracing these components of a compliance program, the guidance also goes further. This expansion likely reflects the influence of Hui Chen, who was hired by the DOJ in late 2015 as a compliance expert.

Chen has said she considers “the smallest details that manifest themselves in the company’s daily operations” when assessing a compliance program, adding that “strong compliance must be data driven.” Those sentiments are clearly manifested in the guidance, which places a new emphasis on measuring how organizations identify and meet compliance objectives.

The compliance guidance does not refer to the widely discussed anti-bribery management system that the International Organization for Standardization issued in the fall of 2016. This system, known as ISO 37001, stresses a number of themes that are picked up in the new guidance, including specific details on the measurement of risk assessment, the duties of management and compliance function staff, and documentation of compliance actions taken.<sup>7</sup>

Nor does the guidance mention compliance standards being developed by other countries. For example, the U.K. Ministry of Justice’s guidance concerning the compliance defense under the U.K. Bribery Act 2010 allows companies to avoid liability for bribery in certain circumstances if they have an appropriate compliance program; Italy has long had a compliance defense; and new Brazilian, French and South Korean anti-bribery laws provide for some form of a compliance defense or have a compliance requirement.<sup>8</sup>

The DOJ mentions none of these standards, and there is no assurance that complying with any or all of them will help a company that is negotiating with the DOJ.

## KEY FEATURES OF THE GUIDANCE

### *Emphasis on process*

Perhaps the most noteworthy characteristic of the compliance guidance is its emphasis on process: The DOJ wants not simply an assertion that a company has achieved an objective, but a demonstration of how the objective was achieved.

The sentencing guidelines and FCPA guide, for example, raise questions about what kind of policies a company has. The compliance guidance goes a step further and asks what the process was for designing the policies, who was involved and which business units were consulted.

To take another example, it may no longer be satisfactory to present slides in a DOJ meeting that say: “The company has an autonomous compliance function. The chief compliance officer has a direct line to senior management and the board, and the compliance function has adequate resources.”

The guidance presents questions that attempt to compel a company to demonstrate that such an assertion is valid, such as:

- How often does the compliance function meet with the board of directors?
- Are members of senior management present for those meetings?
- Who reviewed the performance of the compliance function, and what was the review process?

*The guidance is comprised of 119 questions.*

*Autonomy of the compliance function, an issue that has long been a concern of the DOJ, is stressed.*

- Who has determined compensations/bonuses/raises/hiring/termination of compliance officers?
- Have there been specific instances where compliance raised concerns or objections in the area in which the wrongdoing occurred?
- Have there been times when requests for resources by the compliance and relevant control functions have been denied? If so, how have those decisions been made?

### **Support claims with data**

Implicit in the guidance's demand for a demonstration of the process the company has undertaken to meet its compliance objectives is the need to document the efforts a company has taken to meet those objectives.

The guidance often explicitly seeks documentation or other evidence of some effort to measure results. For example, it asks what "information or metrics" the company used to detect misconduct, how the company measured the effectiveness of its training, and how the company collected and analyzed reports from its hotline or other reporting mechanism.

It further asks whether the company records the number and types of disciplinary actions, requests specific examples of promotions or other benefits or awards that were denied due to compliance and ethics considerations, and seeks information relating to third parties that have been suspended, terminated or audited as a result of compliance issues.

### **Greater sophistication and detail**

The guidance is comprised of 119 questions. To address compliance and remediation questions raised by the DOJ, companies will likely have to present a more nuanced compliance presentation than they have in the past. Companies entering settlement discussions with the DOJ will have to consider whether they will address all of the questions — and, if not, what they will say if they are asked some of those questions.

An appropriate answer may be that certain segments of questions are inapplicable (e.g., "We don't have answers for questions about third parties because we don't use third parties for sales, for interactions with government officials, or for any other high-risk endeavors."), but companies will have to be prepared to explain why certain questions are not relevant to their business.

### **FCPA compliance**

The guidance is not limited to the FCPA, and the DOJ's Chen has stressed that her task is not limited to FCPA compliance. Most of the guidance questions could relate to, say, a sanctions compliance program or the compliance function generally.

On the other hand, as demonstrated by the existence of the FCPA guide, the FCPA pilot program and FCPA enforcement actions that discuss compliance failures,<sup>9</sup> the DOJ seems to focus on FCPA compliance. Indeed, a number of the guidance questions appear to be specifically directed at corruption concerns.

For instance, the guidance has questions concerning how the misconduct in question was funded, whether there has been guidance and training for people "who issue payments," and a series of questions on third parties.

It also includes questions on the rationale for the use of a third party, the existence of contract terms specifying the services to be provided, whether third parties performed the services for which they were paid, and whether the third party is paid fair market value.

All these questions focus principally on corruption risk, and no other compliance topic appears to merit that kind of attention in the guidance.

### **SUMMARY OF THE GUIDANCE**

The guidance's 11 sections, discussed separately below, each contains a series of questions the DOJ may ask corporations attempting to negotiate a settlement related to corporate misconduct.

### ***Analysis and remediation of underlying misconduct***

The compliance guidance starts with the “big picture,” asking for a root cause analysis,<sup>10</sup> if there were any prior chances to detect the wrongdoing (e.g., audit reports) and “why those opportunities were missed.”

#### ***Senior and middle management***

The guidance addresses “conduct at the top,”<sup>11</sup> asking for “concrete actions” that management has taken to lead compliance and remediation efforts and discourage misconduct. It also asks how the company assesses management’s compliance role.

Turning to middle management, it seeks information on the role of leaders from various departments, including finance, procurement, legal and human resources, and it asks how compliance information is shared within the company.

The board’s role is examined with questions regarding compliance expertise on the board itself, private board sessions with officials from the compliance function, and the nature of the compliance information received by the board.

#### ***Autonomy and resources***

The DOJ proposes questions concerning whether the compliance function was involved in training and decisions related to the misconduct, and then seeks information about the compliance function generally.

For example, it asks whether compliance staffers receive the same pay and status as other company officials and whether they are involved in strategic and operational decisions. The DOJ even seeks detailed information as to the turnover rate for compliance and other control function staff (e.g., legal, finance, audit).

The guidance stresses the need for autonomy with respect to the compliance function, an issue that has long been a concern of the DOJ. The agency wants to know if the compliance and control functions can directly report to the board and senior management, how frequently they meet with the board, and who reviews their performance.

If there are no direct reporting lines to the board and senior management, companies may be asked to explain how their compliance and control functions retain independence.

Again, the guidance suggests process questions in an attempt to pinpoint the true independence and authority of the compliance group (i.e., have requests for compliance resources been denied? If so, how were those decisions made?).

#### ***Policies and procedures***

In this section, the DOJ goes well beyond asking whether the company under investigation has compliance policies. It seeks to understand how those policies were designed, whether business units were consulted in that process, how the policies are implemented, and whether anyone is held accountable for their implementation.

In addition, the guidance proposes questions regarding training for those approving payments or proposals and asks whether the policies have been communicated to employees and third parties.

The guidance also focuses on the specific misconduct, asking what controls failed or were missing and whether those errors have since been rectified.

#### ***Risk assessment***

The guidance proposes asking what methodology was used to identify risks, what information the company used to detect the misconduct in question, and how that information informed the company’s compliance program.

This section also discusses how the risk assessment process “accounted for manifested risks.” The meaning of “account[ing] for manifested risks” is not entirely clear, but presumably the DOJ wishes to evaluate the effectiveness of the company’s system for assessing its risks.

### ***Training and communication***

The guidance proposes questions about who receives training in the organization and whether the training is appropriate given the risks faced by different categories of employees.

In addition, it proposes questions about how the company made determinations regarding the nature and recipients of the training and whether there has been an effort to evaluate the training’s effectiveness.

The guidance raises questions about how management has informed employees of its view on the misconduct and how employees are generally informed of misconduct. It suggests that anonymous descriptions of the legal or policy violations may be disseminated to employees.

This line of questions, of course, is in tension with the natural tendency of some companies to keep many allegations or incidents of misconduct strictly confidential, especially if the misconduct will not be disclosed to law enforcement authorities.

In addition, the guidance proposes questions about avenues for employees to ask questions about compliance policies and how the company has assessed whether its employees know when to — or are even willing to — seek advice.

### ***Confidential reporting and investigation***

The compliance guidance assumes that a company will have some form of hotline, which is a clear indication that companies without a reporting mechanism are likely to lose at least some credit in any DOJ assessment of their compliance programs.

The guidance offers questions on how a company reviews reports to its hotline and whether the compliance function has had “full access” to hotline reports and information on investigations.

The implication here is that all information on investigations should be shared with the compliance function. This is a position that may conflict with the practice of some companies to, at least in certain instances, restrict information on investigations to counsel and senior management.

This section also poses questions about the proper scope and independence of investigations, whether investigation findings have been used to shape compliance remediation, and whether investigations probe the role of senior management.

### ***Incentives and disciplinary measures***

Here the DOJ seeks to understand not only how employees were disciplined, but who decided upon the discipline and when that discipline occurred (presumably attempting to assess whether the discipline was meted out only when it became clear that the misconduct would be revealed to the public or the government).

Again, the questions turn to the responsibility of managers, whether they were held accountable for actual misconduct, and any supervisory failures that allowed misconduct to occur. The guidance poses questions about any history of discipline for the type of misconduct under review.

The guidance also discusses the broader implications of incentives for ethical behavior at the company, asking whether the company considered possible “negative implications” of its system of incentives. Presumably, this line of questions seeks to ascertain whether, say, excessive sales bonuses prompt employees to engage in risky behavior.

This section also asks for specific examples of employees receiving or losing benefits (e.g., promotions) due to compliance considerations.

### ***Continuous improvement, periodic testing and review***

The compliance guidance offers a series of general questions on whether audits and reviews of internal controls have been conducted, and how the company responded to the findings of those audits and control testing.

The questions also seek to test why the audits and reviews did not discover or prevent the misconduct. There are also specific questions directed at the frequency of reviews of compliance policies and practices and how those policies are working in specific segments or subsidiaries.

### ***Third-party management***

A series of questions address issues related to controls over third-party relationships. These include third-party risk assessment, the rationale for using the third party, the existence of contract terms describing the specific services to be performed, whether payment terms are appropriate, controls that check whether third-party work actually was performed, monitoring of third parties, and training third-party relationship managers.

With respect to any specific misconduct, the guidance raises the obvious issues: Were there red flags in third-party diligence, and did anybody do anything about them?

This section also addresses whether similar third parties have been terminated or audited for compliance issues and whether there are procedures that prevent terminated third parties from being rehired.

### ***Mergers and acquisitions***

The final section is directed at M&A risks and the nature of the pre-signing diligence and post-close compliance integration efforts, and whether pre-signing diligence informed the post-close compliance process.

## **IMPACT OF THE GUIDANCE**

The compliance guidance is likely to influence DOJ enforcement and corporate compliance in several ways.

### ***DOJ settlements***

The most obvious and direct impact of the guidance will be on parties engaged in settlement discussions with the DOJ. When seeking leniency, companies will generally want to ensure that they have addressed the matters raised by the guidance as thoroughly as possible before opening negotiations with the agency.

### ***Self-disclosure decisions***

Most self-disclosure decisions will now have to be guided, at least in part, by the implications of the compliance guidance. Obviously, if a company has difficulty providing answers that reflect well on its compliance, it may be less likely to disclose its wrongdoing.

Thus, the DOJ's stringent compliance standards may create a perverse incentive to discourage self-reporting. On the other hand, if company management feels comfortable answering the guidance questions, it may be more likely to self-disclose misconduct.

### ***SEC corporate settlements***

It remains to be seen whether the SEC will, in practice, adopt the DOJ's guidance. But it is likely that the SEC will begin to ask companies, if not the exact questions set forth in the guidance, at least those types of questions.

It is worth noting, however, that the SEC did not join in the publication of the DOJ guidance — even though it did so with respect to the FCPA guide.

## Compliance

The guidance emphasizes that the DOJ will make “an individualized determination” when evaluating specific compliance programs, and that the guidance is not a checklist. Despite those assurances, for many companies — and not solely those engaged in DOJ negotiations — the guidance will likely form at least the basis for a checklist.

Addressing the issues raised by the DOJ questions after misconduct occurs will often be difficult (e.g., “Have business units/divisions been consulted prior to rolling ... out [compliance policies]?”), and it is unlikely that a company will be able to satisfy one of the factors the DOJ considers when deciding whether to grant leniency for corporate malfeasance — an appropriate pre-existing compliance program.<sup>12</sup>

Moreover, while many of the guidance’s questions address specific misconduct, many others concern company-wide compliance issues. Compliance officers may reasonably ask themselves whether they can afford to ignore the dozens of questions in the guidance that concern the operation of the compliance function generally.

And if a compliance officer chooses to ignore a guidance question, how does that officer explain a compliance failure relating to that question? Thus, the impact of the guidance on compliance departments will likely be substantial — and could lead to increased compliance costs.

For all of these reasons, the compliance guidance will likely have a substantial impact on the resolution of DOJ corporate enforcement actions and corporate compliance generally.

## NOTES

<sup>1</sup> U.S. DEP’T OF JUSTICE, CRIMINAL DIV., FRAUD SECTION, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, <https://www.justice.gov/criminal-fraud/page/file/937501/download>. The date of the publication of the Compliance Guidance is unclear; there was no news release announcing its publication.

<sup>2</sup> INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL STANDARD, ISO 37001, ANTI-BRIBERY MANAGEMENT SYSTEMS – REQUIREMENTS WITH GUIDANCE FOR USE (2016) (“ISO 37001”). See also, e.g., INTERNATIONAL CHAMBER OF COMMERCE, COMMISSION ON CORPORATE RESPONSIBILITY AND ANTI-CORRUPTION, ICC RULES ON COMBATTING CORRUPTION (2011); OECD, GUIDELINES FOR MULTINATIONAL ENTERPRISES (2011); THE WOLFSBERG GROUP, WOLFSBERG ANTI-CORRUPTION GUIDANCE (2011); TRANSPARENCY INTERNATIONAL, BUSINESS PRINCIPLES FOR COUNTERING BRIBERY: GUIDANCE DOCUMENT (2004); WORLD ECONOMIC FORUM, PARTNERING AGAINST CORRUPTION; PRINCIPLES FOR COUNTERING BRIBERY (2004); WORLD BANK GROUP, INTEGRITY COMPLIANCE GUIDELINES.

<sup>3</sup> U.S. SENTENCING GUIDELINES MANUAL § 8C2.5(f) (U.S. SENTENCING COMM’N 2013); Amendments to the Sentencing Guidelines, Policy Statements, and Official Commentary (proposed Apr. 30, 2004, effective Nov. 1, 2004) (allowing for leniency for an effective compliance program).

<sup>4</sup> U.S. DEP’T OF JUSTICE, U.S. ATTORNEYS’ MANUAL § 9-28.000 – Principles of Federal Prosecution Of Business Organizations.

<sup>5</sup> U.S. DEP’T OF JUSTICE, CRIMINAL DIV. & SEC. ENF’T DIV., A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT, 57-63 (2012). While not mentioned in the guidance, in April 2016, the DOJ released an FCPA pilot program that offered leniency to companies that violated the FCPA if, among other things, they engaged in remediation, which is effectively defined by the standards set forth in the sentencing guidelines.

<sup>6</sup> OECD, GOOD PRACTICE GUIDANCE ON INTERNAL CONTROLS, ETHICS AND COMPLIANCE (2010); OECD, UN OFFICE ON DRUGS AND CRIME, AND THE WORLD BANK, ANTI-CORRUPTION ETHICS AND COMPLIANCE HANDBOOK FOR BUSINESS (2013).

<sup>7</sup> See ISO 37001, § 4.5 and Clause A.4 (risk assessment), §§ 5.1.2, 5.3.1 (management’s role), § 5.3.2 and Clause A.6 (compliance function), § 7.5 and Clause A.17 (documentation). While it is also not mentioned, the guidance appears to draw on the internal control framework described in the Committee of Sponsoring Organization of the Treadway Commission, Internal Control – Integrated Framework (2013).

<sup>8</sup> See Bribery Act, §§ 7, 9; U.K. Ministry of Justice, The Bribery Act 2010; Guidance about procedures which relevant commercial organization can put into place to prevent person associated with them from bribing (2011); Italian Republic, Decreto Legislativo 8 giugno 2001, n. 231 (It.); Federative Republic of Brazil, Clean Company Act, Law No. 12,846/2013, § 7, VIII; Law No. 2016-1691 on transparency, fight against corruption and economic modernization, art. 17; Republic of Korea, Improper Solicitation and Graft Act, Act No.13278, 27, § 24 (2015) (Enforcement Date 28 Sept. 2016).

<sup>9</sup> See, e.g., Information, *United States v. Jerds Lux. Holding S.À.R.L.*, No. 17-cr-7 (D.D.C. Jan. 12, 2017) (FCPA violation alleged when parent did not implement controls to ensure that its Mexican subsidiary would have a written contract with its customs broker or receive anti-corruption representations from its customs broker).

<sup>10</sup> The use of the term “root cause analysis” may be a reference to an ordinary sense of “root cause” (i.e., the underlying or fundamental cause of some event), or it may be a reference to an entire discipline emanating from the management profession. See, e.g., PAUL F. WILSON, LARRY D. DELL, & GAYLORD F. ANDERSON, *ROOT CAUSE ANALYSIS; A TOOL FOR TOTAL QUALITY MANAGEMENT* 9 (ASQ Quality Press 1993): “Root cause is that most basic reason for an undesirable condition or problem which, if eliminated, would have prevented it from existing or occurring. ... Root causes usually are defined in terms of specific or systemic factors. ... Root cause analysis refers to the process of identifying these causal factors, whether it be informal or structural in approach. ... [C]are must be taken to distinguish symptoms from causes.”

<sup>11</sup> The guidance eschews the standard “tone at the top” terminology found in the FCPA guide and other compliance guidance. This may be because the guidance seeks information on specific activities by senior management that influence the compliance culture.

<sup>12</sup> See Sentencing Guidelines, § 8C2.5(f) (greater leniency if “the organization had in place at the time of the offence an effective compliance and ethics program”).



**James Corsiglia** is a senior attorney at **Cleary Gottlieb** in New York. His practice focuses on litigation, particularly securities fraud and other criminal and corporate investigations.