Characteristics Of An Effective Compliance Program

By Stuart H. Deming

Increasingly, in the United States and abroad, the focus has been on controlling corporate behavior through the use of compliance programs. In effect, corporate entities, both for-profit and non-profit, are being encouraged to self-police their behavior by instituting compliance programs.[1] To encourage the implementation of effective compliance programs, the United States and many other countries now require corporate entities to implement and actively enforce compliance programs.

Today, the effectiveness of a compliance program is a critical factor that the U.S. Department of Justice takes into account when exercising prosecutorial discretion, including charging decisions and sentencing recommendations. In the context of anti-bribery compliance programs under the Foreign Corrupt Practices Act ("FCPA"),[2] they have led to declinations and certainly lesser penalties. Under the UK Bribery Act, they may constitute an affirmative defense.[3]

A. Hallmarks of an Effective Compliance Program

In 2012, the U.S. Department of Justice and U.S. Securities and Exchange Commission issued guidance about the FCPA in a publication entitled *A Resource Guide to the U.S. Foreign Corrupt Practices Act* ("*FCPA Guide*").[4] According to the *FCPA Guide*, "hallmarks" of an effective compliance programs are as follows:[5]

1. Commitment from Senior Management and a Clearly Articulated Policy against Corruption[6]

Stuart H. Deming

An effective compliance program requires senior management to have "clearly articulated [entity] standards, communicated them in unambiguous terms, adhered to them scrupulously, and disseminated them throughout the organization."[7]

2. Code of Conduct and Compliance Policies and Procedures

Effective codes of conduct "are clear, concise, and accessible to all employees and to those conducting business on the [entity's] behalf."[8] They must be conveyed in the local language. In tailoring policies and procedures to circumstances associated with an entity and the business it conducts, a compliance program should "outline responsibilities for compliance within the [entity], detail proper internal controls, auditing practices, and documentation policies, and set forth disciplinary procedures."[9]

3. Oversight, Autonomy, and Resources

In addition to ensuring that there is "adequate staffing and resources," one or more specific senior members of man-

agement should be designated and assigned the responsibility of overseeing and implementing a compliance program.[10] The senior executive should have "adequate autonomy from management and sufficient resources to ensure that the [entity's] compliance program is implemented effectively."[11] "Adequate autonomy generally includes direct access to an organization's governing authority, such as the board of directors and committees of the board of directors."[12]

4. Risk Assessment

Depending upon the degree to which particular facts and circumstances may increase risks, compliance procedures need to be correspondingly adjusted to address the heightened risk.[13] This may mean, for example, increased due diligence, more frequent internal audits, or the implementation of a range of special measures.

5. Training and Continuing Advice

In a "manner appropriate of the targeted audience," pertinent policies and procedures need to be communicated throughout an entity whether through training or certifications or other appropriate measures.[14] Similar steps need to be taken with agents, partners and collaborating parties. Measures also must be implemented to ensure that timely advice can be provided.[15]

6. Incentives and Disciplinary Measures

An entity's compliance program must be applied throughout the entity.[16] No one should be exempted from its application. Disciplinary procedures must be clear and applied consistently and promptly.[17] Incentives for compliance should be encouraged.[18]

7. Third-Party Due Diligence and Payments

As part of its "risk-based" due diligence, the qualifications and associations of third parties must be understood as well as the business rationale for using the third party.[19] Third parties are individuals and entities that are not directly owned or controlled by an entity but may act on its behalf. They can take many forms, such as agents, consultants, or representatives, and may also include suppliers, vendors, and distributors. Compliance obligations should be disclosed and commitments obtained from the third parties.[20] Follow-up steps should ensure that the business reasons for using the third party are supported by the terms of any agreements, by the timing and manner in which payments are made, and by there being a verification of the work performed.[21] Third-party relationships should be monitored on an ongoing basis.

8. Confidential Reporting and Internal Investigation

A compliance program should include a mechanism for suspected misconduct to be reported on a confidential basis.[22] Policies should also be implemented to ensure that no one making a confidential disclosure fears retaliation.[23] Adequate resources should be provided so that allegations can be properly investigated and appropriate measures taken.

9. Continuous Improvement: Periodic Testing and Review

A compliance program must be regularly tested and reviewed to identify weaknesses, to adjust to changing circumstances and risks, and to develop ways of improving its efficiency and effectiveness.[24]

10. Mergers and Acquisitions: Pre-Acquisition Due Diligence and Post-Acquisition Integration

To avoid legal and business risks, compliance requires that due diligence be performed as part of mergers and acquisitions.[25] The acquired entity should be fully integrated with the internal controls and compliance program of the acquiring entity.[26] This would extend to all aspects of compliance, such as evaluating and monitoring third parties, training employees, and expanding audits.

B. Evaluation of Corporate Compliance Programs

In December 2017, the Department of Justice issued a policy titled "Evaluation of Corporate Compliance Programs" to further encourage entities to implement effective compliance programs. It continued the Department of Justice's efforts to emphasize the importance of self-disclosure, cooperation, and compliance programs in the resolution of enforcement actions and even the declination of prosecutions. The policy provided greater clarity as to the factors that are taken into consideration in evaluating the effectiveness of a compliance program.

In April 2019, the policy was updated. The update, which is commonly referred to as the "Updated Guidance," builds on the factors identified in the 2017 version of the policy and lays out an ever-increasing focus on the realities of what actually takes place. It identifies a number of additional questions that go to heart of whether a compliance program is truly effective in practice. The twelve areas of consideration in the Updated Guidance are designed to address three "fundamental questions" about the effectiveness of a compliance program:[27]

1. "Is the program well designed?"[28]

Part I "discusses various hallmarks of a well-designed compliance program relating to risk assessment, company policies and procedures, training and communications, confidential reporting structure and investigation process, third-party

management, and mergers and acquisitions."[29] Among the related considerations are whether the allocation of resources is based on risk; whether the risk assessment is subject to periodic review; whether training is tailored to an entity's needs; whether the reporting mechanism is anonymous and effective; and whether appropriate controls are in place for monitoring the use of third parties.[30]

2. "Is the program being implemented effectively?"[31]

"Part II details features of effective implementation of a compliance program, including commitment by senior and middle management of autonomy, resources, incentives, and disciplinary measures." [32] Among the other considerations relative to effective implementation is an assessment of conduct at the top, of a shared commitment between senior leadership and middle management, of adequate oversight, of the seniority and stature of the compliance officials, of the adequacy of resources and autonomy of compliance officials, and of the consistency of applying principles associated with compliance in terms of incentives and discipline.[33]

3. "Does the compliance program work in practice?"[34]

"Part III discusses metrics of whether a compliance is in fact operating effectively, exploring a program's capacity for continuous improvement, period testing, and review, investigation of misconduct, and analysis and remediation of underlying conduct."[35] Among the considerations is whether and to what degree the internal audit function is active; whether and to what degree there is a culture of compliance; whether and to what degree internal investigations are conducted by qualified personnel who are dispassionate in getting at the root cause and analyzing the data; and whether and to what degree does management take remedial measures.[36]

C. Third Parties

Entities can and are regularly held liable for conduct committed by others on their behalf. Indeed, in terms of violations of the FCPA, many, if not most, of the prosecutions arise out of conduct of third parties acting on behalf of an entity. Many entities recognize that serious issues can and do exist with third parties. But they struggle in effectively managing these risks.[37] In this context, implementing an effective anti-corruption due diligence process on third parties as well as continued monitoring of their activities are critical to reducing risk.

1. PACI Working Group

In 2011, the World Economic Forum's Partnering Against Corruption Initiative ("PACI") launched a working group charged with developing Good Practice Guidelines on Conducting Third Party Due Diligence.[38] PACI recognized that in all regions "stricter laws to combat bribery" were being introduced and that enforcement of the laws was on the rise.[39] The "extraterritorial reach of anti-corruption laws [meant] that organizations doing business and raising capital in multiple jurisdictions can be prosecuted for acts of bribery committed anywhere in the world."[40]

Of particular import to the working group was "the prevention of indirect corruption through third parties."[41] Entities "may indeed be held liable for acts of corruption by their third parties, i.e. their agents, consultants, suppliers, distributors, joint-venture partners, or any individuals or entity that has some form of business relationship with the company."[42] The guidelines sought to help "organizations mitigate the risk of becoming involved in corruption through third parties."[43]

Entities following best practices categorize third-party relationships into higher, medium, and lower risk. These categories are generally based on the type of business model. The higher-risk category is more likely to include third parties that are not regulated and only function as introducers of business. A third party that interacts with government officials is also considered higher risk. On the other hand, where third parties are subject to rigorous regulation, they are more apt to fall into a lower-risk category.

2. Increased Accountability for Higher Risks

A responsible senior official needs to be given clear responsibility for overseeing compliance concerns associated with the use of third parties. The absence of having someone responsible and ultimately accountable for third parties creates greater risk. The following scenarios can put an entity at greater risk:

- Having third parties supervised by contractors or other intermediaries with no employees of the entity accountable for the third party's conduct.
- Having long-standing third-party relationships under a contract that was executed before more rigorous corruption compliance controls were implemented.
- Having individuals overseeing third-party relationships that do not insist upon progress reports or other deliverables as contractually required.
- Having third parties operate in foreign markets with limited oversight and control.

In addition, the need for accountability becomes particularly important when familial, economic, or political circumstances position a third party as the only practical option in a particular locality. In such situations, third parties may have undue leverage and may be more likely to disregard an entity's compliance obligations.

3. Third-Party Risk Assessment

In assessing risk, the level of scrutiny should correspond with the level of risk. If later challenged, an entity should be able to demonstrate with confidence that "it is dealing with a *bona fide* third party. The higher the risk, the broader and deeper the third-party due diligence should be."[44]

Onboarding Third Parties: Screening and Due Diligence

For the selection of third parties, an effective screening and due diligence process is essential. Best practices dictate that a risk-based approach be applied to third-party due diligence. As part of the onboarding process, and also on an ongoing basis, third parties should be analyzed to assess their risk. Among the myriad of factors to be evaluated are the offered products and services, the customer pool, and the third-party's location and countries of operation. The scope of the screening and due diligence process should then be based on the assessment of risk.

One of the core components of an effective third-party compliance program relates to when an entity determines to work with or take on a third party—often referred to as "onboarding," It is a time when an entity is most apt to capture complete third-party information. Critical documents are assembled that may include licenses, certifications, and contracts. As part of the onboarding process, it is vitally important that assessments are made of the level of risk and degree of monitoring that will be required.

Ongoing Review

The due-diligence process for third parties does not end with onboarding. Risks must continue to be identified and appropriate due diligence conducted. Uninterrupted third-party monitoring and screening is the key to helping entities reduce risks and potential problems. In the context of international business, screening should continue against global sanctions lists as well as global regulatory, law enforcement, and watch lists. Similarly, adverse media reports should be monitored relating to politically exposed persons ("PEPs") and state-owned enterprises.[45]

Subcontracted services

In monitoring third parties, the oversight process must track whether products and services are actually provided by the third parties and whether they have been sub-contracted to a fourth party.[46] Fourth parties must always be among the considerations as part of the screening and risk-management processes.[47]

Tone at the Top

Senior management and an entity's board of directors are ultimately responsible for the risks of third-party relationships. Depending on the level of risk that the third party may present, approval by senior management should be required. Any delegation of approval authority should not be solely based on monetary thresholds. Consideration of risk should be a factor in whatever delegation of authority may be involved.

Appropriate Investment and Staffing

A sufficient investment in resources, which includes staffing, is essential to managing and monitoring third-party risk. It must not be limited to regulatory compliance. It extends to providing sufficient resources to adequately assess risks and actively manage third parties at the local level as well as from a central location.

Evaluate the Adequacy of the Third Party Process

Procedures need to be put in place to evaluate whether a compliance program is effective. On a regular basis, the program should be carefully evaluated to determine whether risks are being identified and properly mitigated. Well-defined metrics should be developed to assess the effectiveness of the compliance program. Third-party information should be retained in a central location to facilitate oversight, accountability, monitoring, and risk management.

Technology

Technology can play a vital role in managing third-party relationships. It can dramatically impact the efficiency of managing third-party information.[48] This, in turn, enhances the monitoring, the assessment of risks, and the due diligence process associated with multiple third parties. Ultimately, an entity's ability to ensure a greater degree of compliance is increased.

D. The Continuing Evolution

Especially with the global reach of the FCPA and the UK Bribery Act, the trend internationally for entities to self-police is expected to grow. As evidenced by the U.S. Sentencing Guidelines and the Updated Guidance, corporate compliance programs are not limited to issues associated with the bribery of foreign officials. They extend to countless compliance issues.[49] Indeed, as suggested by the Delaware Chancery Court in *Caremark*, the absence of an effective compliance program may now have implications in a civil context for members of boards of directors.[50]

About the Author

Stuart H. Deming *is a principal with Deming PLLC with offices in Washington, D.C. and Michigan. Prior to entering private practice, Mr. Deming served with the U.S. Department of Justice and the Securities and Exchange Commission. He is the*

author of Oxford University Press' Anti-Bribery Laws in Common Law Jurisdictions*, the American Bar Association's (ABA)* Designing An Effective Anti-Bribery Compliance Program: A Practical Guide for Business*; the co-author of the ABA's* The FCPA And UK Bribery Act: A Ready Reference for Business*, and the author of the ABA's* The Foreign Corrupt Practices Act and the New International Norms.

Endnotes

1 A complex matrix is established by the U.S. Federal Sentencing Guidelines for determining fines based upon the culpability of the offender. U.S.C.G., app. § 8A1.1 (2020). In light of the U.S. Supreme Court's decision in United States v. Booker, 543 U.S. 220 (2005), and its progeny, the U.S. Federal Sentencing Guidelines are to be treated as advisory by federal courts in the United States. Yet, even with the cessation of their mandatory status, the U.S. Federal Sentencing Guidelines, and the principles associated with their provisions, continue to play a significant role in the sentencing process, especially with respect to organizations. Relevant factors in assessing culpability include the existence of an effective compliance program.

2 Foreign Corrupt Practices Act of 1977, Pub. L. No. 95-213, 91 Stat. 1494 (1977) (codified as amended at 15 U.S.C. §§ 78m, 78dd-1 to -3, 78ff (2020)) [hereinafter FCPA]).

3 Bribery Act, 2010, § 7 [UK Bribery Act].

4 Criminal Div., U.S. Dep't of Justice & Enf't Div., U.S. Sec. & Exch. Comm'n, A Resource Guide to The U.S. Foreign Corrupt Practices Act 12 (Jan. 16, 2015)

5 *Id.* at 57-63

6 *Id.*

7 *Id.*

8 *Id.*

9 *Id.* at 58.

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.* at 58–59.

14 *Id.*

15 *Id.*

16 *Id.*

17 *Id.*

18 *Id.* at 59–60.

19 *Id.* "As part of an effective compliance program, a company should have clear and easily accessible guidelines and processes in place for gift-giving by the company's directors, officers, employees, and agents." *Id.* at 16. "Proper due diligence and controls are critical for charitable giving. In general, the adequacy of measures taken to prevent misuse of charitable donations will depend on a risk-based analysis and the specific facts at hand." *Id.* at 19.

20 *Id.* at 60–61.

21 *Id.* at 60.

22 *Id.*

23 *Id.*

24 *Id.* at 61–62.

25 *Id.*

26 *Id.*

27 Criminal Div., U.S. Dep't of Justice, Evaluation of Corporate Compliance Programs (2019) [hereinafter Updated Guidance].

28 *Id.*

29 Press Release, U.S. Dep't of Justice, Criminal Division Announces Publication of Guidance on Evaluating Corporate Compliance Programs (Apr. 30, 2019) [hereinafter Criminal Division Announces Publication].

30 Updated Guidance, *supra* note 27, at 2-9.

31 *Id.* at 9.

32 Criminal Division Announces Publication, *supra* note 29.

33 Updated Guidance*, supra* note 27, at 9-13.

34 *Id.* at 13.

35 Criminal Division Announces Publication*, supra* note 29.

36 Updated Guidance*, supra* note 27, at 13-17.

37 The political climate in many foreign countries makes it crucial to take multiple factors into account when vetting third parties. For example, individuals or entities at odds with a political regime are sometimes subject to false charges and adverse state-owned media when they fall out of favor.

38 *Good Practice Guidelines on Conducting Third Party Due Diligence*, The World Economic Forum, at 4 (2013), http://www3.weforum.org/docs/WEF_PACI_ConductingThirdPartyDueDiligence_Guidelines_2013.pdf.

39 *Id.* at 5.

40 *Id.*

41 *Id.*

42 *Id.*

43 *Id.* at 4.

44 *Id.* at 7.

45 *See id.* at 11. Screening data providers may be able to furnish real-time alerts and data feeds on third parties.

46 *Id.* at 6.

47 *Id.* at 12.

48 *Id.* at 10.

49 *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996).

50 *See also* Stone v. Ritter, 911 A.2d 362 (Del. 2006).