THE GUIDE TO COMPLIANCE

SECOND EDITION

Editors
Johanna Walsh, Alejandra Montenegro Almonte and Alison Pople KC

Guide to Compliance

Second Edition

Editors

Johanna Walsh

Alejandra Montenegro Almonte

Alison Pople KC

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK
© 2023 Law Business Research Ltd
www.globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at September 2023, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-257-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Ankura Consulting Group, LLC

Baker McKenzie

Beccar Varela

Cloth Fair Chambers

Davis Polk & Wardwell LLP

Debevoise & Plimpton LLP

Demarest Advogados

Freshfields Bruckhaus Deringer

Galicia Abogados, SC

Herbert Smith Freehills

Jenner & Block LLP

Miller & Chevalier Chartered

Mishcon de Reya LLP

QEB Hollis Whiteman Chambers

Ropes & Gray International LLP/R&G Insights Lab

Wells Fargo

Publisher's Note

The Guide to Compliance is published by Global Investigations Review (GIR) – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing. We tell our readers everything they need to know about all that matters in their chosen professional niche.

Thanks to GIR's position at the heart of the investigations community, we often become aware of gaps in the literature first. *The Guide to Compliance* is a good example. For, although there has been significant growth in guidance on compliance worldwide – and a change in attitudes towards compliance on the part of enforcers (namely that 'good' compliance programmes can still fail) – to date, there has been no systematic guide to how exactly compliance fits into the enforcement equation, or how an organisation can demonstrate that it took compliance seriously. This book aims to solve that.

It combines a systematic *tour d'horizon* of the rules in place around the world with specific practical advice and a scan of the horizon in parts two and three. As such, it should swiftly earn a position in the front row of our readers' libraries.

The guide is part of GIR's steadily growing technical library. This began seven years ago with the first appearance of the revered GIR *Practitioner's Guide to Global Investigations*. *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to do or think about at every stage. Since then, we have published a series of volumes that go into more detail than is possible in *The Practitioner's Guide* about some of the specifics, including guides to sanctions and to monitorships. I urge you to seek out all of them.

If you are a GIR subscriber, you will have received a copy already, gratis, as part of your subscription. If you are not, you can read an e-version at www.globalinvestigationsreview.com.

Last, I would like to thank the editors of *The Guide to Compliance* for bringing us this idea and for shaping our vision, and the authors and my colleagues for the elan with which it has been brought to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher-at-large, GIR
September 2023

Part I

Global Compliance Requirements and Enforcement

CHAPTER 3

US Compliance Requirements

Alejandra Montenegro Almonte, Ann K Sultan and FeiFei (Andrea) Ren[1]

Introduction

Over the past two decades, the US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) – the principal enforcement agencies with jurisdiction over financial and other white-collar crimes – have increased their compliance expectations for corporations through enforcement actions and the issuance of enhanced guidance on designing and maintaining effective compliance programmes. A 2020 Miller & Chevalier survey of corporations measured maturity in the US market as 'most developed', reflecting a trend of companies expanding their compliance programmes beyond 'basic policies' and making meaningful investments to erect robust, sustainable programmes.[2]

Historically, principal compliance guidance came from the United States Sentencing Commission Guidelines Manual (the Sentencing Guidelines). Developed by the Commission to promote effectiveness and fairness in the criminal justice system, as authorised by the Sentencing Reform Act of 1984, the Sentencing Guidelines were amended in 1991 to include Chapter 8, laying out sentencing considerations for organisations that have committed crimes. Subsequently amended in 2004, Chapter 8B, 'Remedying Harm from Criminal Conduct, and Effective Compliance and Ethics Program', outlines the very basic principles deemed most critical by the Commission for evaluating corporate compliance programmes.

---

1 Alejandra Montenegro Almonte is a member and the chair of the international department, Ann K Sultan is a member and the vice chair of the international department and FeiFei (Andrea) Ren is a counsel at Miller & Chevalier Chartered.

2 Miller & Chevalier, 2020 Latin America Corruption Survey, 8 July 2020, www.millerchevalier.com/publication/2020-latin-america-corruption-survey (accessed 31 August 2023).

Further compliance guidance for corporations gradually emerged through enforcement actions brought under the US law prohibiting bribery of foreign public officials: the Foreign Corrupt Practices Act (FCPA). Because the FCPA, unlike more recent anti-bribery laws in other jurisdictions, does not prescribe compliance requirements, the DOJ and the SEC communicate compliance expectations through enforcement actions, such as deferred prosecution agreements and other civil and criminal resolutions with corporations and individuals, and public policy or guidance releases. Together, these sources provide the foundation for many of the elements of corporate compliance that we know today.

Building on years of 'unofficial' compliance guidance through resolution documents, in November 2012, the DOJ and the SEC jointly issued 'A Resource Guide to the U.S. Foreign Corrupt Practices Act' (the Resource Guide), which introduced for the first time the now well-established principles underlying effective compliance programmes. The Resource Guide was updated on 3 July 2020.

In addition, the DOJ has issued other guidelines of its own, such as the guidelines on 'Evaluation of Corporate Compliance Programs' (updated most recently in March 2023) (the Evaluation Guidance) and the 'Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy' (updated most recently in January 2023) (the Enforcement Policy). Although most of the key elements of corporate compliance originated from the Sentencing Guidelines and compliance with anti-corruption laws, these guidelines apply broadly to other financial crimes as well, such as money laundering, fraud, tax evasion and violation of sanctions. In particular, the Evaluation Guidance provides general principles for evaluating the effectiveness of corporate compliance programmes and is not specific to any types of corporate crimes.

In this chapter, we discuss the four main sources of guidance documents on compliance requirements issued by the DOJ. Although the guidance provided does not constitute requirements or obligations mandated by US laws, together these documents define US government expectations and set the standards to which the DOJ and the SEC hold companies when evaluating their compliance programmes in criminal, civil and regulatory enforcement actions.

United States Sentencing Commission Guidelines Manual

The Sentencing Guidelines provide the basis for corporate compliance. Focusing on the need for adequate due diligence and a culture of compliance, the Guidelines state:

> *To have an effective compliance and ethics program . . . an organization shall—*
> *(1) exercise due diligence to prevent and detect criminal conduct; and*

> *(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.*
>
> *Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.*[3]

In a few short sentences, the Sentencing Guidelines provide the framework for later-developed more detailed guidance that dives deeper into compliance programme design, application and testing.

In August 2022, the US Sentencing Commission issued 'The Organizational Sentencing Guidelines' (the Organizational Guidelines), which provide comprehensive organisational sentencing data and summarise the influence of the Sentencing Guidelines over compliance in both the public and private sectors over the past 30 years. Despite the 'widespread acceptance' of the above criteria for 'developing and maintaining effective compliance and ethics programs to prevent, detect, and report criminal conduct', the Organizational Guidelines found that 'the lack of an effective compliance and ethics program may be a contributing factor to criminal prosecutions against organizations', noting that 89.6 per cent of the organisational offenders since fiscal year 1992 did not have any compliance and ethics programme.[4]

A Resource Guide to the US Foreign Corrupt Practices Act

The Resource Guide emphasises the importance of implementing an effective compliance programme that is 'tailored to the company's specific business and to the risks associated with that business' in order to 'prevent, detect, remediate, and report misconduct'.[5] The programme should be 'well-constructed, effectively implemented, appropriately resourced, and consistently enforced'.[6] Having an adequate and effective compliance programme may help companies under

3 US Sentencing Commission, Guidelines Manual, §8B2.1 (2021).

4 US Sentencing Commission, 'The Organizational Sentencing Guidelines, Thirty Years of Innovation and Influence', August 2022 at 2–3.

5 US Department of Justice (DOJ) and US Securities and Exchange Commission, 'A Resource Guide to the U.S. Foreign Corrupt Practices Act', 2nd edn., July 2020 at 56.

6 ibid. at 57.

investigation by the DOJ or the SEC obtain more favourable outcomes in terms of the form of resolution, monetary penalty and compliance obligations that could be imposed.

As a threshold matter, when assessing the effectiveness of a company's compliance programme, the DOJ and the SEC will consider three main factors: whether the programme (1) is well designed; (2) is being applied in good faith; and (3) works in practice.

To guide companies in designing and implementing effective compliance programmes, the DOJ and the SEC introduced 11 'hallmarks' that they consider necessary for a well-functioning compliance programme; however, the DOJ and the SEC acknowledge that one size cannot fit all and, therefore, caution that each company's compliance programme should be designed to address its own 'specific needs, risks, and challenges'.[7] Each of these hallmarks is discussed below.

Commitment from senior management and a clearly articulated policy against corruption

A proper tone from the top is a key component of a strong compliance culture, which is fundamental to a strong compliance programme. The DOJ and the SEC encourage corporate leaders, such as board members and senior executives, to commit to ethical and compliant business practices and to demonstrate that commitment not just through words but by their own conduct. Corporate leaders must ensure that their companies have clearly articulated standards against corruption, which the corporate leaders should unambiguously communicate and disseminate throughout the organisation.

Code of conduct and compliance policies and procedures

A company should have a code of conduct that is 'clear, concise, and accessible' to all employees and its third parties, and that should be reviewed and updated periodically to stay current.[8] To be 'clear, concise, and accessible', a code of conduct should be easy to understand and be relevant to every member of the organisation. It is recommended that companies make their codes of conduct available in the local languages of the countries in which they operate.

Building on the code of conduct, a company should develop and put in place written policies and procedures that 'outline responsibilities for compliance within the company, detail proper internal controls, auditing practices, and

7 ibid. at 58.

8 ibid. at 59.

documentation policies, and set forth disciplinary procedures' to ensure that the principles set out in the code of conduct are followed and that the company can properly manage its specific risks.[9]

The Resource Guide lists a few areas that commonly present compliance risks that a company may need to address through specific policies and procedures, including interactions and transactions with foreign officials; engagement of third parties; gifts, travel and entertainment expenses; charitable and political donations; and facilitating and expediting payments.

Oversight, autonomy and resources

To monitor the implementation of a compliance programme, the Resource Guide calls for a company to assign oversight responsibility to its senior executives, who 'must have appropriate authority within the organization, adequate autonomy from management, and sufficient resources' to ensure the effectiveness of the compliance programme.[10] Whether the resources that a company dedicates to compliance are sufficient will be highly dependent on the company's size and industry, the countries in which it operates, the complexity of its business and risks associated with its business.

Risk assessment

The Resource Guide recommends a risk-based approach to compliance, meaning that a company should analyse the specific compliance risks that it faces and design its compliance programme to address those specific risks, including by dedicating more resources to markets, transactions and third parties that pose higher risks. When the risks for corruption or other financial crimes increase, a company should increase its due diligence efforts, which again are company-specific.

The Resource Guide identifies common factors that often affect those risks, including the countries and industry in which the company operates, the nature of the business opportunity or transaction, the involvement of business partners and other third parties, the level of interactions with governments and the amount of government regulation and oversight.[11]

9 id.
10 id.
11 ibid. at 60.

Training and continuing advice

For a compliance programme to be effective, all levels of officers and employees within a company must understand the company's compliance requirements and how those requirements apply to them. To achieve this goal, a company should conduct periodic training sessions on company policies and procedures and applicable laws. Training should include practical tips and case studies relevant to the specific audience. Similar training may also need to be provided for third parties with which the company does business, particularly in high-risk countries.

In addition to formal training, a company should encourage employees to seek guidance and ongoing compliance advice from company compliance personnel. To facilitate that guidance, a company should ensure that employees know to whom they should reach out for advice and how to do that.[12]

Incentives and disciplinary measures

A company should clearly articulate that compliance obligations apply to all members of the organisation without exception and should implement appropriate procedures to discipline those who fail to follow applicable laws or company policies and procedures. Not only can effective disciplinary measures punish the wrongdoers and remediate their wrongdoing to some degree, from which a company under investigation by the DOJ or the SEC may earn credit, they can also deter others from engaging in misconduct. Appropriate disciplinary measures may range from coaching, written warnings, withholding of discretionary bonuses, exclusion from promotion opportunities or dismissal.

On the other hand, awarding compliant behaviours can further drive and promote corporate compliance, which also shows the value that an organisation places on ethics and compliance. Companies, therefore, should also design incentives to reward those that demonstrate commitment to compliance. Incentives can be monetary, such as making compliance a metric for salary or bonus determination, or non-monetary, such as personnel evaluations and promotions or rewards and recognitions within the organisation.[13]

Third-party due diligence and payments

Third parties remain the highest compliance risks for companies – agents, consultants and sales partners, among others, are frequently involved in cross-border financial crimes. Due diligence provides an effective way to mitigate those risks.

12 ibid. at 60–61.

13 ibid. at 61.

The Resource Guide provides the following three guiding principles on conducting due diligence on third parties, noting that 'the degree of appropriate due diligence may vary based on industry, country, size and nature of the transaction, and historical relationship with the third party':[14]

- First, a company should understand the qualifications and associations of its third parties, including whether they have any relationship with foreign officials.
- Second, a company should have a business rationale for involving a specific third party in a transaction and specify its role and responsibilities in the engagement within the contract terms.
- Third, a company should undertake continuing monitoring after a third party is engaged, including conducting due diligence refreshers periodically based on its risk level, providing compliance training, requesting compliance certifications and exercising audit rights.[15]

Confidential reporting and internal investigation

Companies must investigate allegations of wrongdoing and should design an adequate allegation management system that has (1) a process that allows company personnel and third parties to report suspected or actual misconduct anonymously, and (2) a process for the company to timely and thoroughly investigate the allegations and document its findings and responses, including any disciplinary measures or remedial actions taken.[16]

Continuous improvement: periodic testing and review

The DOJ and the SEC encourage companies to conduct regular testing and review of their compliance programmes and make improvements that may be necessary because of changes in their business operations, applicable laws and regulations, and industry standards.[17]

Pre-acquisition due diligence and post-acquisition integration

In mergers and acquisitions, it is crucial that a company conduct appropriate pre-closing and post-closing due diligence and risk assessment and integrate the new entity into the company's compliance programme in a timely manner. These

14 ibid. at 62.
15 id.
16 ibid. at 66–67.
17 id.

measures will mitigate the risk of potential liability for the company that could result from any misconduct in which the target company might have engaged prior to the transaction.[18]

Investigation, analysis and remediation of misconduct

The Resource Guide calls responding to misconduct the 'truest measure of an effective compliance program'.[19] Companies should implement and maintain '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' and then properly document their responses, including any disciplinary or remedial measures taken.[20] Companies should also analyse the root causes of the misconduct and integrate the lessons learned into their policies, training and internal controls.[21]

Evaluation of Corporate Compliance Programs

The DOJ Criminal Division issued in 2017 (and subsequently amended in 2019, 2020 and 2023) its Evaluation Guidance to assist federal prosecutors in evaluating the effectiveness of a company's compliance programme as part of their enforcement determinations in line with the requirements of the Justice Manual Section 9-28.300 and the Sentencing Guidelines. The Justice Manual requires prosecutors to consider certain factors in determining 'the adequacy and effectiveness of the corporation's compliance programme at the time of the offense, as well as at the time of a charging decision' and the corporation's efforts 'to implement an adequate and effective corporate compliance program or to improve an existing one'.[22]

The Evaluation Guidance retains the hallmark principles introduced in the Resource Guide but crafts questions that federal prosecutors should consider, both at the time of the offence and at the charging or resolution stage, to evaluate whether a company's programme meets the DOJ's expectations for each hallmark. These questions also serve as an important tool for companies seeking to design and maintain an effective compliance programme that meets the expectations of the US authorities.

---

18 id.

19 ibid. at 67.

20 id.

21 id.

22 DOJ Criminal Division, 'Evaluation of Corporate Compliance Programs' (updated March 2023) at 1.

The Evaluation Guidance is organised around three core questions and the compliance hallmarks under each question to help federal prosecutors and (by extension) companies understand how the various hallmarks interact:

Is the compliance programme well designed?	Is the compliance programme being applied earnestly and in good faith?	Does the compliance programme work in practice?
Risk assessment	Commitment by senior and middle management	Continuous improvement, periodic testing and review
Policies and procedures	Autonomy and resources	Investigation of misconduct
Training and communications	Compensation structures and consequence management	Analysis and remediation of any underlying misconduct
Confidential reporting structure and investigation process		
Third-party management		
Mergers and acquisitions		

Building on the Resource Guide, the Evaluation Guidance applies a broader lens to compliance: it seeks first to capture a company's general approach to its compliance programme, and then to focus on a company's application of its programme, and finally to how the programme did or did not work in connection with the alleged misconduct under investigation. A few aspects of the Evaluation Guidance are of particular note.

Emphasis on decision-making rationale

The Evaluation Guidance reflects increased sensitivity to the circumstances and business realities of companies. For example, in its introductory paragraphs, the DOJ notes that certain portions of the Evaluation Guidance may be more or less relevant to companies depending on their specific circumstances: 'In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.'[23]

The Evaluation Guidance drives this point by including questions intended to prompt prosecutors to enquire about a company's rationale for decision-making regarding the design and implementation of its compliance programme – both broadly and at a more detailed level. For example, the section covering continuous

23 ibid. at 2.

improvement, periodic testing and review prompts prosecutors to enquire not only whether internal audits occurred, but also as to the company's rationale supporting its process for determining where and how frequently audits occurred.

Language included in the section on autonomy and resources regarding whether compliance personnel have non-compliance responsibilities drives at the same point. In its discussion of mergers and acquisitions, rather than assuming that a company will conduct all due diligence prior to an acquisition, the DOJ explicitly acknowledges that may not be the case, adding the following question: 'Was the company able to complete pre-acquisition due diligence and, if not, why not?'[24] These enquiries do not preclude a company from choosing a particular course but, rather, suggest that a company should be prepared to defend the rationales that informed programme design and resource allocations.

Focus on programme integration

The Evaluation Guidance prompts prosecutors not only to determine whether certain elements of the programme exist, but also how they work in concert with other components of the programme and are integrated into the day-to-day rhythms of the company. For example, the Evaluation Guidance not only references the importance of having comprehensive policies and procedures, but also prompts prosecutors to ask how the policies and procedures are reinforced through a company's internal control systems.

Increasing emphasis on the use of data to track and test

In a few areas of the Evaluation Guidance, the DOJ emphasises its expectations regarding data collection and use. In discussing autonomy and resources, a section on data resources and access asks whether any impediments exist 'that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?'[25] This may signal both the value the DOJ sees in data as a necessary tool for monitoring and testing compliance programmes, and an awareness of the European Union's General Data Protection Regulation and other restrictions that have come into force in recent years, which can limit access to data for international companies. The Evaluation Guidance also makes clear the DOJ's expectations that companies gather operational data across the company and on employee access to policies. These data points feed into updates to risk assessments and evaluate access to governing documents, respectively.

24 ibid. at 8.

25 ibid. at 11.

In March 2023, the DOJ revised the Evaluation Guidance to update its expectations on the management of corporate data on employees' personal devices and when using third-party applications, especially those with end-to-end encryption or auto-delete features. Overall, the Evaluation Guidance states that company policies on these issues 'should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company'.[26] Prosecutors will consider factors such as the types of electronic communication channels used by company employees in different countries and any company policies that ensure preservation of data and communications in various situations, such as ephemeral message deletion settings, replacement of company devices and use of personal devices under, for example, bring-your-own-device policies.

Focus on the evolution of compliance programmes

Throughout the Evaluation Guidance, the DOJ emphasises both a company's own efforts to evolve its compliance programme and the Department's understanding of that evolution. With respect to the company's own efforts, the Guidance includes new language in the section on risk assessment under 'Lessons Learned', asking: 'Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?'[27] Further, in its discussion of continuous improvement, periodic testing and review, under 'Evolving Updates', the DOJ guides prosecutors to ask: 'Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?'[28] Both questions highlight the importance of learning from internal and external issues and of incorporating that learning into the programmatic changes.

The Evaluation Guidance also makes clear the DOJ's interest in understanding the reasoning behind the evolution of a company's compliance programme. In the introduction to the Evaluation Guidance, the DOJ states that it will be specifically evaluating compliance programmes at multiple points in time: 'both at the time of the offense and at the time of the charging decision and

26 ibid. at 17.
27 ibid. at 3.
28 ibid. at 16.

resolution'.[29] The Guidance emphasises this point by the following addition under 'Risk Assessments': 'In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.'[30] For companies on the receiving end of questions from the DOJ, documentation on changes to their compliance programme – including the 'why' behind changes – will be critical.

Operationalising continuous improvement

Across various sections, the Evaluation Guidance prompts prosecutors to evaluate how a company measures programme effectiveness. For example, the document emphasises in several places the importance of capturing and tracking data to analyse trends and missed opportunities.

Additional explanatory text encourages prosecutors to go beyond simply asking if a programme and its elements are effective, and instead prompts them to ask how that effectiveness is measured in practice. For example, the section on training and communications prompts prosecutors to ask how training effectiveness is measured and improved. In the context of 'continuous improvement, periodic testing and review', the Evaluation Guidance prompts prosecutors to enquire how and how often the company's compliance culture is measured and how that analysis is used to inform the continuous improvement of the company's programme.

Risk assessment as the starting point

The Evaluation Guidance emphasises that:

> *The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.*[31]

Notably, the Evaluation Guidance does not mention 'manifested risks' (a focus in an earlier guidance document) but instead highlights the importance of 'risk-tailored resource allocation' (i.e., 'Does the company devote a disproportionate

29 ibid. at 2.

30 id.

31 id.

amount of time to policing low-risk areas instead of high-risk areas . . . ?'),[32] as well as the importance of updates and revisions to a company's risk assessment and policies and procedures 'in light of lessons learned'.[33] Companies can expect prosecutors to spend more time understanding how risk assessments inform resource allocations, and to scrutinise those decisions. Of course, a company can rightly hope that this line of questioning, in some cases, may lead the DOJ to determine that a specific incident of misconduct in one area does not render the compliance programme ineffective or poorly designed.

Guidance on reporting mechanisms and investigation response

The Evaluation Guidance includes questions about whether a company has established and publicised an anonymous reporting mechanism, underscoring the DOJ's concerns regarding retaliation against reporting of compliance issues. In addition, it includes enquiries about the timing and quality of the company's responsiveness to the results of investigations and the remediation of identified issues. It also underscores the importance of tracking and learning from investigation results (consistent with the Guidance's more general theme of capturing and tracking data to inform continuous improvement).

Proactive justification of business rationales for third parties

The Evaluation Guidance's section on third-party management assesses how the company ensures appropriate business rationales for the use of third parties, more generally. These questions evidence the view that the first, and arguably most important, step in managing compliance risk posed by third parties is to evaluate whether there is a clear business need to engage them and, if so, to articulate the qualifications required to meet that need. Companies will be well served to consider whether their compliance programmes require this step and, if so, whether it is documented and maintained as part of due diligence.

Importance of compensation incentives and clawbacks

In the latest revisions to the Evaluation Guidance in March 2023, the DOJ continues to emphasise compensation to drive compliance. In a retitled section on 'Compensation Structures and Consequence Management' (previously 'Incentives and Disciplinary Measures'), the Evaluation Guidance defines 'consequence management' processes as 'procedures to identify, investigate, discipline

32 ibid. at 3.

33 ibid. at 16.

and remediate violations of law, regulation, or policy'.[34] Specifically, it directs prosecutors to consider whether a company has incentivised compliance by designing compensation systems and non-financial incentives (e.g., promotions and rewards) that are tied to conduct consistent with the company's values and policies, including by asking questions about, for example, the percentage of executive compensation that is 'structured to encourage enduring ethical business objectives' and the role the company's compliance team has in 'designing and awarding financial incentives at senior levels of the organization'.[35]

In addition to compensation incentives, the Evaluation Guidance also instructs prosecutors to consider whether a company has 'policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee'.[36] This consideration is further reinforced by the three-year 'Compensation Incentives and Clawbacks Pilot Program' (the Clawbacks Pilot Program) that the DOJ put in place in March 2023, whereby the DOJ can provide 'possible fine reductions [to companies] where companies seek to recoup compensation from culpable employees and others'.[37] The Clawbacks Pilot Program sets out several considerations and requirements for companies that seek to avail themselves of this potential benefit.

Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy

In January 2023, the DOJ issued the revised Enforcement Policy, formerly known as the 'FCPA Corporate Enforcement Policy,' which applies to all corporate criminal matters handled by the Criminal Division.[38] The revised Enforcement Policy continues to offer companies the presumption that the DOJ will decline prosecution if (1) they voluntarily self-disclose misconduct, fully cooperate with the government's investigation and remediate in a timely and appropriate manner the compliance failures, and (2) there are no 'aggravating circumstances involving the seriousness of the offense or the nature of the offender'.[39]

---

34 ibid. at 12–14.

35 id.

36 ibid. at 13.

37 DOJ, 'The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks', 3 March 2023.

38 DOJ, 'Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy' (updated January 2023) (the Enforcement Policy) at 1.

39 id.

The Enforcement Policy defines 'aggravating circumstances' to include 'involvement by executive management of the company in the misconduct; a significant profit to the company from the misconduct; egregiousness or pervasiveness of the misconduct within the company; or criminal recidivism';[40] however, even where aggravating circumstances are present, a company may still secure a declination if it (1) made a voluntary self-disclosure 'immediately upon the company becoming aware of the allegation of misconduct', (2) had 'an effective compliance program and system of internal accounting controls' in place at the time of the misconduct and disclosure; and (3) provided 'extraordinary cooperation' to the DOJ and undertook 'extraordinary remediation.'[41] The Enforcement Policy does not define what the DOJ considers to be 'extraordinary' cooperation and remediation, but a senior DOJ official noted that prosecutors will consider the 'immediacy, consistency, degree, and impact' of the company's cooperation in making prosecuting decisions'.[42]

Previously, companies were required to disclose 'all relevant facts known to [them], including all relevant facts about all individuals substantially involved in or responsible for the violation of law'.[43] The Enforcement Policy now broadens the self-disclosure obligation and requires companies to disclose 'all relevant, non-privileged facts known to [them], including all relevant facts and evidence about all individuals involved in or responsible for the misconduct at issue, including individuals inside and outside of the company regardless of their position, status, or seniority'.[44]

In addition, the DOJ also 'encourages self-disclosure of potential wrongdoing at the earliest possible time, even when a company has not yet completed an internal investigation, if it chooses to conduct one.'[45] When evaluating a company's

40 id.

41 ibid. at 2.

42 DOJ, 'Assistant Attorney General Kenneth A. Polite, Jr. Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy', 17 January 2023, www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-georgetown-university-law (accessed 8 August 2023). For example, prosecutors can consider whether a company cooperated immediately from the start of an investigation, consistently told the truth and provided evidence that might be otherwise unobtainable; and whether the assistance provided by the company led to certain results, such as 'testifying at a trial or providing information that leads to additional convictions'.

43 DOJ, 'FCPA Corporate Enforcement Policy' (updated March 2019) at 2.

44 Enforcement Policy at 3.

45 id.

self-disclosure, the DOJ will 'make a careful assessment of the circumstances of the disclosure, including the extent to which the disclosure permitted the Criminal Division to preserve and obtain evidence as part of its investigation'.[46]

The Enforcement Policy also continues to emphasise proactive, rather than reactive, cooperation, requiring companies to inform the DOJ 'where the company is or should be aware of opportunities for the [DOJ] to obtain relevant evidence not in the company's possession and not otherwise known to the [DOJ]'.[47] The Enforcement Policy makes it clear that if a company claims that disclosure of data is prohibited or restricted by foreign law, it must establish the existence of those prohibitions or restrictions and identify 'reasonable and legal alternatives to help the [DOJ] preserve and obtain the necessary facts, documents, and evidence for its investigations and prosecutions'.[48]

Conclusion

The expansion of compliance guidance issued by the DOJ and the SEC and the increasing depth of that guidance signals to US and foreign corporations a heightened expectation of proactive and considered compliance programme development. Collectively, the guidance documents noted provide a blueprint for companies seeking to develop and enhance their compliance programmes and for those having to defend their existing programmes.

However, as the various guidelines, and statements by enforcement officials, have made clear, compliance programme design and effectiveness is a particularised and individualised art, where one size does not fit all and continued customisation, evaluation and improvement is the expectation. Companies would, therefore, do well to incorporate the guidance provided into their own internal monitoring and testing efforts to ensure their compliance programme stays relevant to their operations.

46 id.

47 ibid. at 4.

48 id.

The Guide to Compliance is the first guide to tackle the compliance side of the enforcement equation in a systematic way. It combines a *tour d'horizon* of the rules in place around the world with specific practical advice for corporations and their counsel, and a scan of the horizon in parts two and three. It is part of the GIR technical library that has grown out of the *Practitioner's Guide to Global Investigations* and now includes guides to, among other things, monitorships and sanctions.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

ISBN 978-1-80449-257-4