

 **LATIN LAWYER**

THE GUIDE TO CORPORATE COMPLIANCE

THIRD EDITION

Editor

Andrew M Levine

Associate editors

Reynaldo Manzanarez Radilla

Valeria Plastino

Fabio Selhorst

The Guide to Corporate Compliance

Third Edition

Editor

Andrew M Levine

Associate Editors

Reynaldo Manzanarez Radilla

Valeria Plastino

Fabio Selhorst

Reproduced with permission from Law Business Research Ltd
This article was first published in April 2022
For further information please contact insight@latinlawyer.com

Publisher
Clare Bolton

Senior Account Manager
Monica Fuertes Britz

Senior Content Coordinator
Georgia Goldberg

Production and Operations Director
Adam Myers

Production Editor
Simon Tyrie

Subeditor
Jane Vardy

Chief Executive Officer
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK
© 2022 Law Business Research Ltd
www.latinlawyer.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 is accurate as at April 2022, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – clare.bolton@lbresearch.com

ISBN 978-1-83862-863-5

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

Acknowledgements

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

Andrew B Jánszky

Anheuser-Busch InBev

Barbosa Müssnich Aragão

Beccar Varela

Camargo Corrêa Infra

Carey

Debevoise & Plimpton LLP

Davis Polk & Wardwell LLP

FerradaNehme

FTI Consulting

Hogan Lovells

Incode Technologies Inc.

Maeda, Ayres & Sarubbi Advogados

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

McGuireWoods LLP

Acknowledgements

Morrison & Foerster LLP

Ropes & Gray

Skadden, Arps, Slate, Meagher & Flom LLP

Sullivan & Cromwell LLP

TozziniFreire Advogados

Vinson & Elkins, LLP

Von Wobeser y Sierra, SC

Publisher's Note

Latin Lawyer and LACCA are delighted to publish the third edition of *The Guide to Corporate Compliance*.

Edited by Andrew M Levine, a litigation partner at Debevoise & Plimpton LLP, with the assistance of associate editors Reynaldo Manzanarez Radilla, a corporate attorney and compliance professional, Valeria Plastino, vice president, general counsel and regional compliance officer at Lumen Technologies, and Fabio Selhorst, senior vice president of corporate affairs at Hapvida, this new guide brings together the knowledge and experience of leading practitioners from a variety of disciplines and provides guidance that will benefit all practitioners.

We are delighted to have worked with so many leading individuals to produce *The Guide to Corporate Compliance*. If you find it useful, you may also like the other books in the Latin Lawyer series, including *The Guide to Mergers and Acquisitions* and *The Guide to Restructuring*, as well as our jurisdictional references and our new tool providing overviews of regulators in Latin America.

My thanks to the editors for their vision and energy in pursuing this project and to my colleagues in production for achieving such a polished work.

Contents

Introduction 1
Andrew M Levine

PART I: SETTING THE SCENE

1 The Evolution of Compliance: How Did We Get Here? 13
Peter Spivack and Isabel Costa Carvalho

2 Latin America's Compliance Climate Today..... 37
Julie Bédard and Mayra Suárez

PART II: BUILDING AN EFFECTIVE COMPLIANCE PROGRAMME

3 The Profile of a Successful Compliance Department 85
Reynaldo Manzanarez Radilla

4 Developing a Robust Compliance Programme in Latin America.... 99
Brendan P Cullen and Anthony J Lewis

5 The Board's Role in Compliance..... 123
Andrew B Jánszky

6 Best Practices for Conducting Compliance Risk Assessments 159
Daniel S Kahn, Tatiana R Martins and Jordan Leigh Smith

7 Building Effective Internal Communication Channels and
Adapting Employee Compliance Training 174
María González Calvet, Krystal Vazquez and Baldemar Gonzalez

8	Third-Party Due Diligence: Expanding a Compliance Programme to Suppliers and Clients	194
	Palmina M Fava, Zachary Terwilliger and Natalie Cardenas	
9	How to Conduct Internal Investigations of Alleged Wrongdoing.....	209
	Adrián Magallanes Pérez and Diego Sierra Laris	
10	Embracing Technology.....	226
	Matt Galvin, Jaime Muñoz and Dheeraj Thimmaiah	

PART III: COMPLIANCE AS A BUSINESS ADVANTAGE

11	Selling Integrity	247
	Jussara Rocha Tibério	
12	Assessing and Mitigating Compliance Risks in the Transactional Context	259
	Andrew M Levine and Erich O Grosz	
13	The Advantages of a Robust Compliance Programme in the Event of an External Investigation.....	275
	Shin Jae Kim, Renata Muzzi Gomes de Almeida, Giovanni Paolo Falchetta, Karla Lini Maeji, Fabio Rawet Heilberg, Brunna Padovan Ortega de Almeida and Laís Neme Cury Augusto Rezende	

PART IV: LEGISLATIVE AND REGULATORY PRESSURE POINTS

14	Anti-Money Laundering and Counter-Terrorist Financing in Latin America	297
	Rafael Collado González, Lucía Álvarez Galvez, Josefa Zamorano Quiroga and Camilo León Millones	
15	Navigating Competition Rules	308
	Lorena Pavic, José Pardo, Benjamín Torres and Raimundo Gálvez	

- 16 Demonstrating Compliance with Data Privacy Legislation 331
Devika Kornbacher, Palmina M Fava, Gabriel Silva and Chris James
- 17 Reducing Cyber and Data Risk through Incident Readiness
and a Culture of Compliance..... 347
Antonio Gesteira, Jordan Rae Kelly and Adriana Prado
- 18 Understanding and Mitigating US Sanctions Risks in
Latin America 357
Ryan Fayhee, Diego Durán de la Vega, Tyler Grove and Anna Hamati

PART V: STAYING COMPLIANT IN HIGHER-RISK INDUSTRIES

- 19 Working with the Public Sector: How to Say 'No' to Bribery..... 375
Anna Carolina Malta Spilborghs and José Guilherme Berman
- 20 Risk Management in the Financial Services Industry
in Argentina and the Changes Being Adopted..... 386
Maximiliano D'Auro and Gustavo Papeschi

PART VI: TRENDS TO WATCH

- 21 The Creep of Legislation Targeting Private Corruption..... 407
Ben O'Neil and Elissa N Baur
- 22 External Compliance Monitorships 424
Erica Sellin Sarubbi and Tomás Fezas Vital Mesquita
- 23 Compliance as a Foundation for ESG Oversight 440
Juliana Gomes Ramalho Monteiro, Thiago Jabor Pinheiro and
Marcel Alberge Ribas

24 ESG in Latin America and the Rise of the Social Pillar 452
Ruti Smithline, Hayley Ichilcik, James M Koukios, Stephanie Pong and
Lauren Navarro

About the Authors 465

Contributors' Contact Details..... 495

Part II

Building an Effective Compliance Programme

CHAPTER 6

Best Practices for Conducting Compliance Risk Assessments

Daniel S Kahn, Tatiana R Martins and Jordan Leigh Smith¹

Introduction

Latin America has for many years been an area of focus for US regulatory agencies, and that focus is only growing. To use a salient example, improper payments to government officials in Latin America have constituted an increasingly large proportion of criminal and civil actions brought by US authorities under the US Foreign Corrupt Practices Act (FCPA), from roughly a third of FCPA actions arising from misconduct in Latin America in 2016, to more than 70 per cent in 2021.

Companies seeking to mitigate these legal and regulatory risks should implement an effective compliance programme designed to prevent and detect criminal conduct and non-compliance with corporate policies and procedures. To design such a programme, it is essential to understand the risks unique to each company and tailor the compliance programme to address those risks. Even when misconduct occurs, the existence of a compliance programme that is thoughtfully designed to address a company's specific risk profile and periodically updated is considered by regulatory authorities to be a critical mitigating factor when determining potential penalties for legal violations.

¹ Daniel S Kahn and Tatiana R Martins are partners, and Jordan Leigh Smith is counsel at Davis Polk & Wardwell LLP. The authors would like to thank associate David Feinstein and law clerk Nicole Intrieri for their assistance in the preparation of this chapter.

Importance of risk assessment

The starting point for designing any compliance programme

Expectations of what constitutes an effective compliance programme are well developed, particularly in the United States. The degree to which a company meets those expectations is often a significant factor in the outcome of criminal or regulatory investigations of alleged misconduct or other non-compliance. While there is no ‘one-size-fits-all’ compliance programme, regulators – in particular, the US Department of Justice (DOJ) and US Securities and Exchange Commission (SEC) – have promulgated different standards for assessing whether a specific programme is effective.

This includes articulating ‘hallmarks’ that provide detailed guidance to companies on how to implement a programme that addresses certain key principles, starting with how the company has identified, assessed and defined its risks, and the degree to which the programme devotes appropriate scrutiny and resources to the spectrum of risks.² A well-designed legal and regulatory compliance programme therefore should be grounded both in preventing and mitigating risks, and also in documenting the process through which risks are identified, monitored and addressed.

Overview of the risk assessment process

Organisations conduct assessments to identify a number of different types of enterprise risks, including strategic, operational, financial and compliance. Within that overall approach, a compliance risk assessment seeks to identify risks relating to a company’s ability to adhere to applicable legal and regulatory regimes, in order to ensure that appropriate controls are in place to reduce the likelihood or scope of a violation and corresponding regulatory action.

Understanding a company’s geographic and operational footprint, and how that footprint interfaces with the relevant regulatory regimes, is the necessary starting point for any compliance risk assessment process. This will enable the company to understand the general compliance risk profile of its organisation. With this general understanding, the next step in the risk assessment process is to identify the areas of the business that pose a higher likelihood of possibly violating applicable laws, and evaluate the key policies and procedures in place to control for those risks.

2 Evaluation of Corporate Compliance Programmes, Department of Justice Criminal Division (June 2020) (ECCP).

In undertaking this exercise, which is often referred to as ‘risk mapping’, companies consider the likelihood that the risk of violating the law will be realised given current controls, as well as the impact that such a violation would be expected to have on the company. Risk mapping allows companies to identify critical gaps in controls and to determine how to prioritise addressing those gaps based on the actual risks – specifically, the likelihood of a violation combined with the severity of the consequences such a violation would have on the business.

Therefore, an ideal risk assessment process seeks to identify not only the existence of a risk, but the likelihood that it may occur, its relevant vectors to the company’s operations and the potential severity of its impact should that risk materialise. Although companies in the same industry and geographical region may have similar risk profiles, and can often learn from one another regarding various risks, the specific risk profile of every company is inherently unique. A company cannot effectively allocate compliance resources, design policies, procedures and controls, devise trainings for relevant employees and otherwise implement a well-functioning compliance programme absent an understanding of these unique risks.

Appropriately allocate resources and implement practical controls

The adequacy of resources allocated to a compliance programme generally, and to identify risks within that framework more specifically, is another hallmark of an effective compliance programme. The design of a corporate compliance programme should start by asking not just what the relevant risks are and how the company has elected to address them, but whether the compliance programme devotes appropriate ‘scrutiny and resources’ to the risks identified.

A critical aspect of a well-designed compliance programme is having the appropriate focus and resourcing on the areas of highest risk to the company, which depends in part on the initial risk assessment. Tailoring attention and resources on a risk-weighted basis is not only important to allow for internal monitoring of potential compliance lapses, but also can be critical in defending a compliance programme in the US and, increasingly, jurisdictions such as Brazil and other countries in Latin America. As discussed below, in the US, the government gives its prosecutors authority to ‘credit the quality and effectiveness of a risk-based compliance programme’ that devotes resources and attention in a risk-appropriate manner, even where that programme fails to prevent an infraction.³

3 ECCP at 3.

Identifying risk

Determining the inputs

A risk assessment is only as good as the inputs used to identify risk. As noted in the DOJ's Evaluation of Corporate Compliance Programmes (ECCP), an effective risk management programme is designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business.⁴ In determining the likelihood of such misconduct, companies should analyse the risks based on factors such as the location of its operations, the relevant industry, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel and entertainment expenses, and charitable and political donations.⁵ This list is not exhaustive, but should be treated as a minimum standard for conducting a risk assessment.

To align with the ECCP's guidance, those conducting a risk assessment should reflect on the methodology that the company has used to identify and address the particular risks it faces. A company should pay particular attention to the types of information and metrics it has collected and analysed to detect misconduct, and how those metrics have informed the company's weighting of risks and allocation of resources.⁶

Common methods for detecting potential compliance gaps include the use of employee questionnaires and surveys, interviews with subject matter specialists and business operations personnel, and third-party diligence and audit reports. In addition, DOJ guidance specifies that the use of mechanisms for confidential internal reporting of suspected misconduct, and processes for conducting prompt internal investigations of allegations and incorporating lessons learned from those investigations into your risk assessment process, are further hallmarks of an effective compliance regime.

Regulatory officials have increasingly highlighted the need to use data to drive risk assessment and monitoring. As such, an effective compliance model will continually look for ways to quantify risks and monitor compliance. This does not necessarily require the application of sophisticated AI or computer modeling. Though such methods are obviously desirable where appropriate and consistent with a company's resources, core competencies and business model, there are other, less technical opportunities to use data to drive compliance

4 id. at 8.

5 id. at 3.

6 id. at 2-3.

efforts. Quantitative analysis can be applied to key risk assessment metrics like the volume of complaints and the speed of a company's corresponding investigation and resolution. Similarly, while information may be readily available about the volume, frequency and amount of payments to third parties acting on behalf of the company, a quantitative assessment might establish and rely on the application of averages, baselines and other metrics for identifying irregularities.

Common compliance risk vectors

Each company faces its own unique risks, and there is no universal set of criteria for assessing risk comprehensively. However, there are a number of risk vectors that are widely accepted as posing significant compliance risks.

Industry

Certain industries have been historically prone to enforcement actions for compliance failures, such as natural resources extraction and construction or engineering. The concentration of regulatory activity in these industries might be attributed in part to the geographic dispersion of their operations, as well as the frequency of interaction with government officials and state entities. In the extraction industry, obtaining business-critical permits and licences inevitably entails the involvement of government officials at the national, regional and local levels. Similarly, many large construction projects in Latin America are infrastructure projects tendered by government entities and overseen by a relatively small number of key officials.

While certain industries figure more prominently in the history of government compliance enforcement actions, the DOJ and SEC are not limited to enforcement actions in those industries, and indeed are often looking for new areas in which to signal the importance of adherence to the anti-bribery laws. Accordingly, staying abreast of developments in this space remains essential.

For example, WPP plc's 2021 resolution with the SEC stemmed from an alleged bribery scheme regarding improper payments to purported vendors in connection with obtaining government contracts in Brazil, and bribes to fund a political campaign in Peru. WPP, an international advertising and marketing conglomerate, was undertaking an aggressive global expansion by acquiring local companies in high-risk markets within Latin America.⁷ While advertising

⁷ 'SEC Charges World's Largest Advertising Group with FCPA Violations' (24 September 2021), <https://www.sec.gov/news/press-release/2021-191>.

and marketing is less characteristically an industry of focus for anti-corruption actions, its expansion into these markets opened the company up to risks that may not have historically been a touchstone in its industry.

Government touchpoints

As noted above, certain industries have historically been considered high-risk for compliance misconduct because they typically entail a high level of dependence on government permits, approvals and contracts. Dependence on interactions with national or local government inevitably creates a risk of corrupt activity. While observers of the compliance industry will no doubt be familiar with the *Lava Jato* investigation in Brazil and its progeny, more recent notable examples in Latin America include Vitol's resolution with the DOJ over allegations that it bribed officials at Brazil's, Ecuador's and Mexico's state-owned oil companies to receive confidential information and to win government contracts.

To that end, companies that engage in a high percentage of business with state-owned entities or rely on government permits should pay particular care to that aspect of their risk assessments. Beyond the payment of cash bribes, though, care should also be taken in assessing and addressing the risk associated with seemingly more innocuous business practices, such as offers of gifts, entertainment or travel. Though at some level these practices are standard and accepted, they can also be used to influence officials. Companies can mitigate risks associated with business travel and entertainment in many ways, but where such practices are prevalent, an effective risk assessment will seek to understand industry and local customs and regulations in service of detecting irregularities.

Other common red flags to be aware of when considering whether a gift to a government official is appropriate include if the business purpose seems incidental to an entertainment purpose; if the government official is strategically situated to award business to the company; if a travel destination may be perceived as exotic or desirable; if the official's spouse or family members are invited; if expenses are paid to the official personally; or if the official is reluctant or unwilling to get written approval.

Operations or other business conducted in high-risk countries

The Biden administration has recently signaled an increased focus on regions deemed 'high-risk' for compliance misconduct and, in particular, corruption. On 6 December 2021, the administration released the United States Strategy on Countering Corruption as its first major step pursuant to its 3 June 2021

Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest, which outlined a heightened focus on ‘priority’, high-risk countries.

While the administration’s official documents declined to specify which countries qualify, a large proportion of recent anti-corruption resolutions and individual actions have arisen from alleged misconduct in Latin America, including resolutions with Amec Foster Wheeler (Brazil), Vitol (Brazil, Mexico and Ecuador), J&F Investimentos S.A. (Brazil) and Sargeant Marine Inc. (Brazil, Venezuela and Ecuador). In fact, misconduct in Brazil alone was alleged in two of the DOJ’s and SEC’s four foreign corruption resolutions in 2021. Similarly, on 15 October 2021, the DOJ announced a new tip line to receive information regarding potential corruption in the Northern Triangle nations of El Salvador, Guatemala and Honduras.

The administration’s clear focus on high-risk regions, combined with the frequency of enforcement actions and prosecutions predicated on conduct in Latin America, underscore the compliance risk facing companies operating in the region. As a result, such companies should ensure that their risk assessments are particularly mindful of recent regulatory news and developments, and that they have controls in place that reflect lessons learned from those matters.

Nature and extent of use of third parties

Perhaps one of the most critical factors for assessing how well a company evaluates and manages risk relates to its use of third parties such as agents, vendors, distributors and resellers. The ECCP directs prosecutors to assess a company’s third-party risk management practices as a factor in determining whether a given compliance programme is in fact able to ‘detect the particular types of misconduct most likely to occur in a particular corporation’s line of business’.⁸ Similarly, the July 2020 update to the DOJ and SEC’s FCPA Resource Guide (Resource Guide) emphasised that companies must conduct ‘risk-based due diligence’ and monitoring of third parties, which it says are ‘commonly used to conceal the payment of bribes’.⁹ Additionally, the ECCP suggests that regulators will examine whether companies ‘engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process’.¹⁰

8 ECCP at 8.

9 A Resource Guide to the US Foreign Corrupt Practices Act, Department of Justice and Securities and Exchange Commission (July 2020) (Resource Guide), 62.

10 ECCP at 8.

Consequently, ongoing monitoring of third parties, including through such mechanisms as periodic renewal procedures and a risk-based third-party audit programme, are now particularly important for companies that utilise third parties to do business in Latin America. Indeed, the Resource Guide highlights that simply '[r]elying on due diligence questionnaires and anti-corruption representations is insufficient, particularly when the risks are readily apparent'.¹¹ To that end, regulators emphasise the importance of using data analytics to conduct ongoing monitoring of third-party payments for irregularities, and keeping track of data related to third-party due diligence and payments.

With heightened compliance risk stemming from the use of third-party agents, companies should first determine whether there is a clear business need to engage them, and be sure to document its rationale. Third parties and other intermediaries who may interact with government officials on the company's behalf must be carefully evaluated in particular, including through methods such as background and qualification checks, properly monitoring invoices and the methods and amounts of payments, and confirming that contractual protections such as audit rights and termination rights are fully utilised.

Level of M&A activity (including joint ventures)

Companies active in the M&A space must be aware that the DOJ and SEC can and will hold buyers responsible for the past conduct of acquired entities, particularly when that conduct continues post-acquisition. Both agencies have emphasised that well-designed compliance programmes should include comprehensive due diligence of any acquisition targets, but also note that, when robust pre-transaction due diligence proves challenging, prompt post-acquisition diligence is expected and that, in any event, timely compliance system integration is critical.

The Resource Guide recognises the importance of the acquiring entity having 'a robust compliance programme in place and implement[ing] that programme as quickly as practicable at the merged or acquired entity'.¹² The ECCP stresses the need for a 'process for timely and orderly integration of the acquired entity into existing compliance programme structures and internal controls', as well as, 'post-acquisition audits'.¹³ Creating further incentives to conduct in-depth post-acquisition diligence, the Resource Guide explains that the government is less

11 Resource Guide at 65.

12 Resource Guide at 29.

13 ECCP at 9.

likely to pursue enforcement actions against the predecessor company when the successor uncovers and self-reports misconduct at an acquired entity and fully remediates the issue. Thus, it is imperative that companies engaged in M&A activity seek to understand the risks they may be inheriting by conducting fulsome risk assessments (both pre- and post-transaction), as well as timely, risk-based compliance integration.

Ultimately, failure to anticipate corruption and other compliance risks in M&A transactions can have significant legal and commercial consequences. Aside from the risk of regulatory action, business that depends on unknown corrupt practices of the acquired company may be lost when those practices are eventually discovered (ideally through diligence and risk assessment by the acquiring entity). Additionally, contracts obtained through bribes of the acquired company may be legally unenforceable. Lastly, the continued existence of inaccurate books and records, including entries disguising past bribes or other misconduct, may raise the spectre of accounting and internal controls enforcement action directed at the successor entity.

Similarly, joint ventures have figured prominently in enforcement actions and continue to attract regulatory attention. Joint ventures present risks of both M&A transactions and classic third-party business partner arrangements, and joint venture partners may also be liable for taking any action in furtherance of a venture's improper activity, regardless of whether the company controls the joint venture. If a company is a majority owner of a joint venture (typically defined by US regulators as having majority voting power), regulators will expect that company to be in a position to dictate the joint venture company's policies and procedures. However, even non-controlling participants are required to use good faith efforts to exert their influence to prevent violations of law and ensure that an effective compliance programme is in place. As in any transaction, risk assessment and due diligence are paramount, with particular consideration given to the jurisdiction of the proposed joint venture, the business model and nature of the proposed business activity of the venture, the degree of dependence on government contracts, permits, licences and other regulatory actions, and the anticipated frequency of interactions with government officials.

Known issues

Now more than ever, companies with past or pending resolutions should be particularly focused on their risk assessments. In her 28 October 2021 speech, US Deputy Attorney General Lisa Monaco announced that in reaching a corporate resolution, prosecutors should consider 'all prior misconduct . . . whether or not that misconduct is similar to the conduct at issue in a particular investigation'.

This change significantly broadens the scope of prior misconduct now deemed relevant to the terms of a potential corporate resolution, and in so doing emphasises the need for holistic and comprehensive global risk assessments.

Similarly, failures to rectify known issues that are not yet the subject of regulatory action can have significant consequences. In WPP's 2021 resolution with the SEC, the company was cited for failing to promptly or adequately respond to 'repeated warning signs of corruption or control failures at certain subsidiaries'.¹⁴

Existing controls and compliance programme

Part of any risk assessment involves taking a fresh look at a company's existing compliance programme. The risks identified in consultation with compliance professionals and subject matter specialists throughout the company should be mapped and tested against those existing controls. Doing so serves to identify potential areas of weakness in existing controls, as well as create opportunities to leverage or improve them. This may include other risk assessment systems at the company, its internal audit functions, and employee training or issue reporting processes.

At a minimum, testing of existing controls should be conducted with reference to the hallmarks of an effective programme as enumerated in the ECCP and other relevant guidance, as well as industry best practices and local regulator expectations. Particularly in regions deemed to present higher compliance risk, active monitoring of regulatory and industry developments and enforcement actions helps to ensure that a company's programme is not just capable of identifying the appropriate spectrum of risks, but has a documented basis for contesting charges of inadequacy, especially where the government's expectations around compliance programme design may supersede local or regional standards.

US prosecutors are also directed to consider the manner in which the company's compliance programme has been tailored based on its risk assessment. Companies should make use of risk assessments to ensure that they are giving greater scrutiny, as warranted, to higher-risk areas and transactions than more modest and routine transactions. For instance, the ECCP posits that a 'large-dollar contact with a government agency in a high-risk country' is more likely a high-risk transaction than 'more modest and routine hospitality and entertainment'.¹⁵ Beyond that, though, companies are advised to remember that

14 See 'SEC Charges World's Largest Advertising Group with FCPA Violations,' (24 September 2021), <https://www.sec.gov/news/press-release/2021-191>.

15 ECCP at 3.

Careful, documented consideration of factors (including analysis of data gathered from oversight and operations alike) leading to risk-tailoring decisions will later prove useful in maximising any potential leniency the ECCP and other guidance permits prosecutors to exercise, should misconduct occur.

Who conducts the compliance risk assessment

In preparing to conduct or update a compliance risk assessment, what considerations about the structure and authority of that process apply? Put simply, who within the company should conduct compliance risk assessments? Ideally, such assessments are overseen by the company's compliance function, with input from relevant stakeholders within the organisation, including the business and the board of directors. It is critical that the compliance function engage with the business during this process, as the business 'owns' and is most familiar with the risks and related controls as a natural product of their direct involvement in the day-to-day operations of the company. Compliance collaborates with the business to define the risks, provide guidance on legal requirements, and monitor the risks and related controls to ensure the compliance programme is operating as intended.

As a company's key overseers, it is also essential that the board of directors or an appropriate sub-committee are involved in, or at least briefed on, both initial and ongoing risk assessments. When the DOJ resolves a financial fraud or FCPA case, it routinely includes an 'Attachment C' detailing 'Corporate Compliance Programme' requirements to be met in connection with the resolution of the case. Attachment C clarifies that responsibility for the implementation and oversight of a company's compliance code, policies and procedures – including those inherent in conducting a risk assessment – should be assigned to one or more senior executives with authority to report directly to independent monitoring bodies. To ensure the integrity and utility of that reporting line, Attachment C sets forth requirements that include the need to conduct training and effectively communicate policies and procedures not just to officers, employees and agents, but to directors as well.

Periodically updating risk assessments

Importance of renewing risk assessments periodically

While a risk assessment may be the starting point in designing a compliance programme, it is critical to understand that the process of identifying and evaluating legal and regulatory compliance risks does not end with the initial assessment. One of the hallmarks of an effective compliance programme, as enumerated in the ECCP, is that it has procedures for conducting regular and

ongoing risk assessments. The DOJ directs prosecutors to evaluate a company's 'revisions to corporate compliance programmes in light of lessons learned', as an indicator of appropriate risk identification and tailoring.¹⁶ Thus, risk assessment is not an event but a process, one that is actively monitored and evolves over time.

The DOJ and SEC emphasise the importance of renewing risk assessments periodically to prevent a compliance programme from stagnating. Regulators will assess whether a company's periodic risk assessment updates are 'limited to a 'snapshot' in time' or whether updates are also triggered by events and the results of continuous monitoring. Recall that the ECCP allows prosecutors to credit the quality and effectiveness of a risk-based compliance programme that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. As a result, efforts should be made to risk-tailor compliance programmes in light of lessons learned, not only to prevent misconduct, but as evidence of a well-functioning compliance programme. This demonstrates the importance of having a process to document and incorporate lessons learned into an ongoing risk assessment. For example, companies should ensure that they have in place a process for tracking and incorporating into their periodic risk assessments any key takeaways from both their own prior issues and from those of other companies operating in the same industry or region.¹⁷ To the extent companies can promptly risk-tailor their compliance programmes in this way, those efforts can bolster a defence against enforcement action even if misconduct occurs.

Thus, any risk assessment should be subject to periodic review, both cyclically and as triggered by events, to ensure that the programme remains defensible and current. Any compliance programme updates should likewise incorporate new or evolved risks, whether discovered through misconduct or other periodic self-assessment activities.¹⁸

Triggering events for renewed assessment

As indicated, risk assessments should be renewed periodically regardless of whether there is a specific triggering event. However, there are particular events that can warrant an immediate renewal of a risk assessment process or that will be more likely to result in significant changes to the results of your risk mapping. In determining what events should trigger updates to a risk assessment, keep the following in mind.

16 ECCP at 3.

17 *id.*

18 *id.* at 15.

Change in business model, applicable regulatory scheme, or operations

Changes to a company's business model will likely change the company's risks. Take, for instance, a company that formerly dealt exclusively in managing business-to-business payments, but has now expanded to provide consumer-level retail payments. Whereas the company's risk management previously may have relied on tools like audit rights in customer contracts and long-standing experience in customer industry norms and practices, in its new retail venture, these practices may be of limited value.

Additionally, updates or changes to regulatory schemes may alter a company's risk landscape. For instance, the Anti-Money Laundering Act of 2020 (AMLA) expanded the Bank Secrecy Act's definition of 'financial institution' to cover those engaged in the exchange or transmission of 'value that substitutes for currency', such as cryptocurrencies, and added further industries like antiquities dealers, advisers and consultants to the definition.¹⁹ Doing so brings such entities within the nominal purview of extensive money laundering regulations. Coming within the scope of a new regulatory scheme imposes new compliance obligations and therefore compliance risks.

Finally, changes in a company's operations can alter the company's sources of compliance risk. For example, a company that shifts from in-house manufacturing to outsourced manufacturing in foreign countries must now develop a process for identifying new sources of risk, like sanctions risk and risks associated with reliance on foreign government interactions.

Acquisition of new entity

As noted above, companies may inherit the risks of misconduct at acquired companies. Where robust pre-transaction due diligence is possible, an acquiring company can more accurately evaluate a target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Where such diligence is challenging, there is still significant value in prompt post-acquisition efforts to integrate the new business into the compliance function, root out potential compliance failures, and self-disclose them.

¹⁹ AMLA, Section 6102(d).

Importantly, the risk assessment is not only important for the acquiring company in identifying what new exposure it now has, but also in determining how best to implement the company's policies, procedures and controls at the newly acquired entity. It is often the case that the company's compliance programme will need to be right-sized to best fit the newly acquired entity.

Internal misconduct

The existence of newly discovered violations of company policy or law constitutes an important data point for the company's risk assessment. That is, if some employees engaged in misconduct, that is one potential risk that may be exploited again.

As such, each instance of internal misconduct that is identified should inform a company's risk assessment procedures going forward.

Misconduct at companies operating in similar industries or regions

Relatedly, news of alleged misconduct at companies operating in similar industries or regions marks an opportunity to re-evaluate your own risk assessment. Enforcement announcements are typically intended to trigger self-reflection at similarly situated entities. Even beyond their utility in providing information about compliance that regulators deem a high priority, staying responsive to such developments highlights senior leadership's earnestness and good faith, and conveys that an organisation can effectively adapt to changes in the business environment.

For instance, when enforcement activity begins to touch new industries, companies in that industry should expect a higher level of scrutiny and respond accordingly. Recent such signposting by the government includes the aforementioned Strategy on Countering Corruption, which named a number of particular industries that the Biden administration plans to focus its anti-corruption efforts on, including private equity, investment advisers and real estate.

Conclusion

The prospect of accurately identifying and monitoring a spectrum of risks in an ever-shifting business environment may be daunting. However, there are certain touchstone principles upon which companies can consider relying:

- Understand the risks that face the company as a result of its geographic and operational footprint.
- Design the risk assessment with all the relevant data points possible, including data relating to the company's government touchpoints, operations and business in high-risk countries, use of third parties, M&A activity, prior instances

of internal misconduct, and risks that were identified in connection with regulatory actions against other companies operating in the same region or industry.

- Become knowledgeable about regulator expectations, and remain attuned to changes as reflected in guidance and the lessons of recent enforcement actions.
- Look for ways to modernise assessments of risk through data analysis and quantification of relevant inputs.
- Ensure that risk assessments are not only conducted on-cycle, but are responsive to off-cycle developments and triggering conditions.
- Focus on ensuring robust integration of – and communication between – subsidiaries and centralised compliance functions.
- Treat documentation of processes and rationales as if it were as important as the underlying compliance processes. If misconduct occurs, this material will be critical in defending a compliance programme against charges that it was inadequately designed or otherwise dysfunctional.

APPENDIX 1

About the Authors

Daniel S Kahn

Davis Polk & Wardwell LLP

Daniel S Kahn represents companies and individuals in criminal and regulatory enforcement matters and in conducting internal investigations involving violations of the anti-bribery laws, money laundering and securities, commodities, and financial fraud, as well as on compliance matters. A former prosecutor, he served for 11 years in senior roles at the Department of Justice.

The Wall Street Journal described Dan as the DOJ's 'most recognizable expert on the Foreign Corrupt Practices Act'. At the DOJ, Dan was acting Deputy Assistant Attorney General of the Criminal Division and, earlier, head of the Fraud Section and FCPA Unit. He supervised matters involving FCPA violations, money laundering, and fraud related to digital currency, fintechs, commodities, securities, healthcare and procurement.

At the DOJ, Dan played a central role in developing enforcement policies on the FCPA, corporate investigations and resolutions, compliance and monitors. He worked with enforcement authorities in the US, Europe, Asia and Latin America.

Dan teaches Corporate Criminal Investigations at Harvard Law School and Global Anti-Corruption at Georgetown Law Center, and sits on the board of the NYU Program on Corporate Compliance and Enforcement.

Tatiana R Martins

Davis Polk & Wardwell LLP

Tatiana R Martins represents companies and individuals in white collar defense and regulatory enforcement matters and in conducting internal investigations involving violations of the anti-bribery laws, money laundering and financial frauds. She also advises on compliance matters.

An experienced trial lawyer, Tatiana has tried multiple cases to jury verdict. As an Assistant US Attorney for the SDNY, she tried high-profile cases including that of former New York Assembly Speaker Sheldon Silver. As chief of the SDNY Public Corruption Unit, she oversaw major investigations and prosecutions, including cases against Michael D Cohen, NCAA basketball coaches and high-level UN officials.

Tatiana is recognised for her white-collar work by *Chambers USA*, where sources say she ‘has excellent judgment’ and ‘always produces excellent legal analysis without losing sight of the practical and strategic implications’.

Tatiana was born in Recife, Brazil and is a native speaker of Portuguese. She is also fluent in Spanish.

Tatiana is on the boards of the Office of the Appellate Defender and the Tinker Foundation.

Jordan Leigh Smith

Davis Polk & Wardwell LLP

Jordan Leigh Smith advises clients on compliance and anti-corruption matters, including providing advice on civil, criminal and internal investigations relating to alleged violations of the Foreign Corrupt Practices Act (FCPA), fraud and other financial crimes. Her significant experience in compliance includes serving as acting chief compliance officer for a global industrial company.

She assesses compliance programmes, advises on remediation steps and implementation of effective compliance programmes, engages in risk assessments, and advises on corporate governance issues. She conducts due diligence and provides strategic, structural, contractual and risk mitigation advice in connection with M&A, joint ventures, investments and third-party engagements.

Clients also turn to Jordan for practical advice on day-to-day compliance issues, including in connection with contractual negotiations, reviewing policies and procedures, enhancing internal systems and controls, training and disciplinary issues.

Davis Polk & Wardwell LLP

450 Lexington Avenue

New York NY 10017

United States

Tel: +1 212 450 4000

daniel.kahn@davispolk.com

tatiana.martins@davispolk.com

jordan.smith@davispolk.com

www.davispolk.com

Published by Latin Lawyer and LACCA, edited by Andrew M Levine, a litigation partner at Debevoise & Plimpton LLP, with associate editors Reynaldo Manzanarez Radilla, a corporate attorney and compliance professional, Valeria Plastino, vice president, general counsel and regional compliance officer at Lumen Technologies, and Fabio Selhorst, senior vice president of corporate affairs at Hapvida, *The Guide to Corporate Compliance* is designed to assist key corporate decision-makers and their advisers in the effective handling of their compliance obligations in Latin America.

This guide delivers specialist insight to our readers – general counsel, compliance officers, government agencies and private practitioners – who must navigate the region's complex, fast-changing framework of rules and regulations.

In preparing this guide, we have been working with practitioners from a variety of disciplines and geographies, who have contributed a wealth of knowledge and experience. We are grateful for their cooperation and insight.

Visit latinlawyer.com
Follow @LatinLawyer on Twitter
Find us on LinkedIn

ISBN 978-1-83862-863-5