

[Latham & Watkins Litigation & Trial](#) and [White Collar Defense & Investigations Practices](#)

August 15, 2022 | Number 2995

## Empowering Corporate Compliance Functions in a Post-Pandemic Environment

***Building an effective post-pandemic compliance program requires taking stock of, and acting on, US regulators' shifting approach and priorities.***

As detailed in a recent Latham [Client Alert](#), the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC) have issued a number of policy updates and public pronouncements over the last several months, emphasizing the importance of **empowered** and **accountable** corporate compliance programs. US regulators clearly expect compliance programs to be empowered with sufficient resources, personnel, stature, and authority within their organizations to be effective, and they are looking to hold chief compliance officers (CCOs), so-called gatekeepers, and individual bad actors accountable for corporate compliance.

This follow-up Client Alert provides practical guidance for companies seeking to ensure that their compliance teams are empowered and accountable, particularly in the post-pandemic environment, which presents unique challenges for organizations seeking to build a best-in-class compliance program. These recommendations include the following:

- I. [Re-evaluate corporate compliance risks](#)
- II. [Address not just new risks, but also new business realities in the compliance program](#)
- III. [Ensure compliance has the resources to do its job](#)
- IV. [Ensure compliance has the opportunity and ability to do its job](#)
- V. [Use technology as a force multiplier for compliance](#)
- VI. [Do the hard work of evaluating the effectiveness of the compliance program](#)
- VII. [Focus on training gatekeepers and middle management](#)
- VIII. [Ensure the whistleblower hotline is working effectively](#)

Not all of the tips in this Client Alert may be relevant to or necessary for all companies. However, in light of the aggressive enforcement posture that US regulators<sup>1</sup> have taken, their increasingly rigorous assessments of compliance programs, and the clear statements from the DOJ and the SEC about individual accountability and the importance of ensuring that corporate compliance programs are empowered and accountable, companies have real incentives to review and, if appropriate, enhance their existing compliance programs.

## I. Re-evaluate corporate compliance risks

The foundation of any effective compliance program is a thorough understanding of the company's key compliance risks. Indeed, the "starting point" for DOJ prosecutors examining corporate compliance programs is to ask "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."<sup>2</sup> Assistant Attorney General for the Criminal Division Kenneth Polite, Jr. recently underscored this expectation, noting that the DOJ "closely examine[s] the company's process for assessing risk and building a program that is tailored to then match those resources to that specific risk profile."<sup>3</sup>

But for nearly every organization, business today looks quite different from business three years ago. Companies and their employees have changed the way they work; businesses have folded, merged, and transformed; and customer populations, supplier bases, and the competitive landscape have all completely shifted. In light of these fundamental transformations, companies should conduct (or refresh) their compliance risk assessments to understand their post-pandemic compliance risk profile.

Given how business has evolved, effective risk assessments (or re-assessments) could account for the following changes, among other things:

- How employee populations have evolved (including not only total headcount but also how management and other organizational structures, including reporting lines, may have changed)
- How employee behavior and ways of performing work tasks day to day have shifted
- How key customer profiles have changed (including whether there are new or increased numbers of government/state-owned entity customers, customers in new markets, or a change in the direct versus indirect customer ratio)
- Whether new regulatory requirements apply to the business
- What changes, if any, have occurred in the company's supply chain
- Updates to the jurisdictions, functions, and manners in which the company's data is stored, shared, and secured
- Changes in how the company approaches marketing, business development, and other external-facing activities (i.e., travel, lodging, in-person hospitality practices, event sponsorships, etc.)
- Whether the nature of the company's business presents new risks under increasingly strict and ever-evolving anti-money laundering (AML) and sanctions regimes
- Whether there have been changes in financial systems or other technical tools available to the company

## II. Address not just new risks, but also new business realities in the compliance program

Organizations may benefit from ensuring that their compliance programs not only align with their current risk profile, but also account for current business realities in the post-pandemic environment. For example:

- **Third-party risk management.** Third-party risk management presents a unique challenge in a remote or hybrid work environment, as many relevant business processes — including processes that are not led by compliance but are nonetheless important from an ethics and compliance perspective — have been delayed or discontinued because of COVID-related challenges. Historically, quality and procurement teams may have conducted supplier site visits as part of their standard supply chain management activities. For many companies, these visits are on pause, are happening less frequently, or are now handled virtually or outsourced to third parties. Although these site visits were not historically led by compliance, these types of touchpoints with suppliers help ensure that the suppliers are legitimate and qualified, and are providing the contemplated services. To the extent that these (or other) “business-side” controls are discontinued, compliance organizations may want to consider whether additional efforts may be warranted (particularly for vendors that are not subject to diligence managed by the compliance team), such as more robust due diligence, reference checks, site visits, or enhanced vetting of business records.
- **Employee engagement.** Like all post-pandemic business functions, compliance programs need to account for a more transient, remote, and potentially less engaged workforce. To ensure employees stay engaged with compliance, consider the following practices:
  - *Rethinking training programs.* Consistent with recent DOJ guidance, short, tailored training that is digestible, relatable (i.e., includes relevant examples), practical, and engaging is most effective — especially when learners may not be sitting in an office or training room.<sup>4</sup> Potential ways to make training more engaging include: employees starring in short training modules, movie-trailer style segments, opportunities to win small corporate- and/or compliance-branded items, or incorporating buzz phrases, slogans, and even catchy tunes. Compliance organizations may also be able to leverage internal resources beyond legal and compliance — such as marketing, human resources, and corporate branding — to build more engaging training content.
  - *Compliance presence.* In the remote work environment, being “out of sight, out of mind” increases the risk that personnel working remotely fail to follow policies and procedures, either because they simply forget the rules or because they feel disconnected from their company’s compliance culture. As such, compliance has an incentive to think creatively about being “present” as much as possible in front of the business. Consider, as examples: short compliance reminders (including via less traditional tools, such as text message, corporate chat tools, internal message boards, or other informal forms of corporate communication); providing business leaders with compliance speaking points or slides they can work into their regular business meetings; regular compliance role/attendance at town halls or staff meetings; monthly or weekly compliance themes; or periodic updates regarding enforcement trends or recent compliance case studies. (See Topic III below for guidance about ensuring compliance is present across a company’s geographic footprint.)
  - *Branding compliance.* Relatedly, companies could think about branding their compliance programs to embed them into the mindset and culture of the organization. Compliance slogans, a company-specific title for the Code of Conduct, or even a compliance mascot are some examples. This practice is less about making sure that employees understand the company’s

specific rules and more about ensuring compliance is woven into the fabric of the company's culture and becomes second nature to the business, even in the remote/hybrid work environment.

- *Incentivizing and disciplining compliance.* Disciplinary and incentive actions do not have the ripple effect that occurs naturally when people are in the office every day. As such, leaders and compliance functions would benefit from being intentional about ensuring (consistent with privacy requirements and mindful of attendant risks) that employees know that they will be held accountable for misconduct. Similarly, compliance would be well served by finding visible ways to publicly acknowledge individuals who show leadership with respect to ethics and compliance.<sup>5</sup>
- **Refresher training on core compliance processes.** As employees re-engage with in-person business activities, companies may want to get in front of growing pains for employees who may be rusty on the company's compliance protocols, or for employees who have not engaged in field work since they joined the organization. What may have been second nature prior to the pandemic (e.g., submitting timely expense reports, ensuring attendance is recorded in accordance with internal event policies, or seeking pre-approvals for expenses as required under company procedures) may now be forgotten (or never learned). This challenge could be addressed in a short "nuts and bolts" refresher training on key controls to ensure employees are developing good process-oriented habits as they enter the post-pandemic environment.
- **Employee interviews.** During interviews, managers and human resources professionals assess whether a candidate embodies the company's culture — including the company's commitment to ethics and integrity. When conducting in-person interviews, they can do so by observing how the candidate interacts with others, exhibits professional conduct, and other behavioral cues. These intangible qualities — including whether the individual is committed to doing business ethically — are harder to observe in a remote interview. To account for that, companies could consider specifically and proactively asking candidates about their commitment to ethics and compliance during the interview process, such as how they have exhibited that commitment in prior roles, how they would respond to hypothetical situations presenting thorny compliance dilemmas, or otherwise pressure-testing their compliance acumen.

### III. Ensure compliance has the resources to do its job

Companies would be well served by taking a hard look at whether their programs are sufficiently resourced to be effective in light of those risks and to prove to regulators that their programs are appropriately empowered to be effective. A number of elements factor into whether the compliance function is adequately resourced:

- **Qualified and identifiable compliance lead.** The DOJ and the SEC expect a company's compliance function to be led by a qualified internal employee.<sup>6</sup> Depending on the size of the company, this may be in the form of a dedicated CCO (or equivalent title) or a dual-hatted resource who serves as the compliance lead among other functions. Having a designated compliance resource empowers that individual to take a leadership role as it relates to compliance, and makes the idea of compliance more tangible for employees. Regardless of title, a designated compliance person — and their team, as appropriate — should be qualified and experienced enough to handle the role effectively.
- **Local compliance resources.** Particularly for companies with a global footprint, it is critical that compliance teams are visible not just at headquarters but in the regions as well. How companies ensure a global compliance "presence" may vary based on the company's size and risk profile. For some companies, ensuring such presence could mean placing country-level or regional-level

compliance contacts in the field. For other companies, it may be more appropriate to assign a “compliance champion” or “compliance liaison” who is a point of contact locally and works closely with the corporate compliance function. (Benchmarking against peer companies of comparable size and risk can be helpful to ensure that a company’s approach is in line with industry practice.) In any event, local compliance resources will be most effective if they are trained on identifying and escalating red flags, are familiar with key compliance rules and requirements, and have access to relevant corporate compliance personnel.

- **Compensation, titles, and reporting lines.** Another way regulators assess whether the compliance function has sufficient stature is by looking at where the function sits within the organization as well as the compliance team’s compensation. In other words, are compliance leads compensated — in terms of base salary and bonuses — in a way that suggests they are well-respected in the organization?<sup>7</sup> Companies could consider reviewing their compliance team’s compensation packages compared to others in similar functions (taking into consideration experience, tenure, localization, etc.) to ensure that their compensation reflects the company’s prioritization of compliance. This issue also comes up in the context of titles, particularly in hierarchical organizations. Companies may want to assess whether their compliance teams are titled in a way that reflects their stature and authority. Similarly, the DOJ will evaluate reporting structures when assessing the stature of compliance in the organization. Companies seeking to empower compliance could ensure that the compliance function (especially the CCO) has solid and dotted lines commensurate with their standing in the organization; that compliance reports as directly as possible to senior leadership; and that compliance has access to relevant board and management committees.<sup>8</sup>
- **Compliance spend.** If a company is facing a corporate enforcement action, it could be asked to provide regulators with annual budgets for compliance, both for internal resources as well as external spend (e.g., third-party vendors, outside counsel, forensic accounting, data scientists, etc.).<sup>9</sup> There is no magic number, and of course, actual spend could vary based on issues identified in any given year. But companies should be mindful that this dollar amount could be scrutinized by regulators and that they could be well served by benchmarking spend against peers with a similar size and risk profile and by considering any trends over time.

#### IV. Ensure compliance has the opportunity and ability to do its job

US regulators expect compliance to be empowered with the *opportunity* and *ability* to serve as a check on the commercial and operational parts of the business. Compliance cannot operate in a vacuum, but functions best within an organization — and helps mitigate risk — when integrated into key business processes.

US regulators also expect compliance to have more than just an advisory role in these business decisions. In particular, regulators expect compliance to have the authority (whether it be voting rights, veto rights, escalation authority, or otherwise) to challenge the business if and when appropriate. (In Section VI we highlight that testing whether compliance does in fact exercise this power is one way to evaluate the effectiveness of a compliance program.) This integration could come in the form of placing compliance on key transactional review processes or committees, involving compliance in developing internal risk thresholds, and compliance participation in board-level discussions about high-risk transactions.<sup>10</sup>

To ensure compliance has a meaningful opportunity to weigh in, organizations would be well served by involving compliance in important business decisions early in the process. Compliance should be involved before there is so much momentum around the contemplated transaction (because of internal business

enthusiasm, commitments that are made internally, resources expended, etc.) that no one — whether it be compliance or the business — could stop the transaction. Placing compliance as the final reviewer is not the hallmark of compliance having actual authority to divert a planned action or transaction.

Taking it one step further, compliance functions could consider finding ways to identify and plug in on higher risk business transactions (e.g., activities in high-risk markets, challenging customers, third-party relationships that raise question, high-value targets, etc.) well before the review and approval stage. Plugging in earlier in the process would allow compliance to play an active role not just in the approval process, but would create the opportunity for oversight, education, monitoring, and overall risk management process in real time (i.e., before it is too late). One of the most effective ways to do this is leveraging data and analytics to identify high-risk opportunities and prospects early in the process. For further discussion on data analytics, see Section V.

Empowering compliance is not just a US government expectation, but it will be critical for organizations that are going through corporate enforcement actions. With CCO certifications now a mainstay in corporate resolutions with the DOJ,<sup>11</sup> CCOs need access and authority to attest to the efficacy of their organization's compliance program. In fact, that was the point of the CCO requirement in the first place: to effectively force organizations to empower their compliance functions so that the CCOs can make that certification. As Assistant Attorney General Kenneth Polite said in recent remarks, the CCO certification requirement “is intended to empower our compliance professionals to have the data, access, and voice within those organizations to ensure them and the Department that company has an ethical and compliance-focused program.”<sup>12</sup>

## V. Use technology as a force multiplier for compliance

Companies that invest in compliance-related technology are hitting the mark on several US government and industry benchmarks: building a system that will work effectively and efficiently; evidencing to regulators that their program is adequately resourced (see Section III); and introducing tools that allow for constructive use of compliance data and analytics — a compliance best practice and DOJ expectation.<sup>13</sup>

Furthermore, failure to leverage compliance technology may put companies a step behind the government (both in the US and abroad), as many regulatory bodies already use data analytics to detect regulatory and criminal misconduct. These tools have long been leveraged by the SEC in the insider trading context,<sup>14</sup> by the DOJ with respect to healthcare fraud,<sup>15</sup> and by regulators outside the US with respect to government graft and tax evasion,<sup>16</sup> among other uses. Recently, the Biden Administration identified “**leveraging innovation** in the fight against corruption” as a key “strategic objective” for national security.<sup>17</sup> And President Biden promised to mobilize more technological resources to fight corruption, including the Anti-Corruption Solutions through Emerging Technologies program, which will engage diverse stakeholders — spanning government, civil society, and the private sector — to collaborate on tracking, developing, improving, and applying new and existing technological solutions to systemic challenges in preventing and detecting corruption.<sup>18</sup> Assistant Attorney General Polite similarly confirmed that the DOJ uses data analytics to detect and combat criminal schemes. His message to company leadership is to do the same: “consider what data analytics tools you could use to monitor compliance with laws and policies within your own operations and to help ferret out wrongdoing when it occurs[.]”<sup>19</sup>

Companies can leverage technology in their compliance programs in many ways, such as:

- Data analytics around key compliance risk areas (e.g., third parties, gifts and hospitality, accounts payable, discounts and margins, logistics, etc.) to proactively identify trends and outliers in real time and to use that data to drive the direction of the compliance program

- Systems to integrate and automate compliance or business processes (and reduce opportunity for human error and fraud/misconduct)
- Dashboarding that provides management and compliance teams with real-time business and compliance data and metrics (although companies should ensure that the metrics drive action, since dashboarding for the sake of dashboarding may cause more harm than good)

Companies of all types and sizes have and utilize data and analytics for a range of commercial and operational business purposes, much of which can be leveraged by compliance. As more processes are brought online and into the cloud to support hybrid and remote work, compliance teams may similarly be able to leverage these new data sets for compliance purposes.

Companies thinking about incorporating technology into their programs are often overwhelmed. There is no “one size fits all” approach to how companies can integrate data and analytics into their compliance programs. A good starting point is to think about the highest risk area and/or where the organization already has data available (and personnel supporting that data) and leverage that. Companies should not feel pressured to implement a comprehensive compliance data analytics program in one go, but can begin building it piece by piece, prioritizing risks and leveraging available data.

## VI. Do the hard work of evaluating the effectiveness of the compliance program

When prosecutors evaluate the strength of a company’s compliance program, they are directed to ask not just whether the program is well designed, but also: “[d]oes the corporation’s compliance program work in practice?”<sup>20</sup> In other words, companies cannot simply draw up a strong compliance program on paper, “press play,” and consider their work complete.

Companies can only answer that question if they are doing the hard work of evaluating the effectiveness of their compliance program. Assistant Attorney General Polite explained that the DOJ looks closely at “whether the company is **continuously testing the effectiveness** of its compliance program — that it’s improving, that it’s adapting, that it’s updating the program to ensure that its sustainable and adapting to changing risks.”<sup>21</sup>

Companies can take a number of approaches to evaluate their corporate compliance programs; the key is finding ways to honestly and critically assess if the program is actually working. This evaluation can take many forms but often is driven by specific employee feedback, active testing and auditing, or comparison of relevant data over time. Below are examples of ways companies can assess the effectiveness of their compliance programs:

- Employee surveys and exit interviews regarding the compliance program’s effectiveness, independence, and autonomy
- Testing training and policy comprehension by employees (both as part of the training module, but ideally months after a training session or policy rollout)
- Evaluation of employee behavior pre- and post-training or guidance<sup>22</sup>
- Testing the effectiveness of reporting hotlines and investigations (discussed in more detail in Section VIII)

- Third-party controls assessment (including timeline for review/approval of new third parties, compliance with any remediation or controls mandated by compliance, etc.)
- Internal audits specifically targeted to the implementation of the compliance program (i.e., compliance program audits, not just compliance considered as part of general internal audits)
- Data-driven assessment of whether compliance is independent and empowered, such as measuring at what rate compliance exercises its power to reject third parties, transactions, etc.

## VII. Focus on training gatekeepers and middle management

US regulators are increasingly focused on individual liability as a key part of their enforcement strategy, with a particular eye toward compliance “gatekeepers.”<sup>23</sup> This expectation is echoed in the latest version of the DOJ’s Evaluation of Corporate Compliance Programs, which specifically recommends that companies should invest in further trainings for their compliance and controls personnel.<sup>24</sup> Prosecutors are asked to examine the training that those in “relevant control functions” have received and ensure that the company has “provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred.”<sup>25</sup>

In light of this guidance, companies may want to consider developing appropriately tailored training for gatekeepers, which will vary by company but could include finance teams, compliance functions, legal teams, auditors, human resources, procurement leads, and other key gatekeeper roles. This training will be most effective if it goes beyond a “check the box” exercise and gatekeepers find it relevant, actionable, and relevant to their work. (See Section II for guidance on effective training in the remote workplace.)

Companies may similarly want to consider educating and empowering middle management with respect to compliance matters. The DOJ specifically directs prosecutors to “examine how middle management, in turn, have reinforced [compliance] standards and encouraged employees to abide by them.”<sup>26</sup> While tone at the top is important, middle management typically has direct interactions with front-line employees, and thus companies should be mindful of “tone at the middle.”<sup>27</sup> Middle managers can be trained and empowered not only to understand the compliance messages that senior leadership and compliance issues, but also to convey those messages to the people they supervise in a way that resonates with their teams. Further, middle managers are often the first call when employees have compliance-related questions (before calling compliance or human resources or the whistleblower hotline).<sup>28</sup> As such, middle managers would benefit from knowing the answers to common compliance questions, particularly as they relate to basic compliance processes (e.g., documentation, recordkeeping, approvals, etc.). This not only will get employees answers more quickly, but will also reduce the process-related burden on the compliance staff.

## VIII. Ensure the whistleblower hotline is working effectively

Whistleblower hotlines are not new, but they are particularly important in today’s business environment when employees are not always in the office and able to walk down the hall to raise a question or report a concern. Part of a well-designed compliance program is establishing (and publicizing to employees) a confidential reporting mechanism whereby employees may report or seek guidance regarding potential or actual misconduct without fear of retaliation.<sup>29</sup> But with employees working remotely (in whole or in part), compliance teams are challenged to think creatively about how to advertise the hotline beyond traditional posters in the break room. Consider, for example:

- Embedding links into firm-wide emails or signature blocks



- Sending reminders via non-traditional corporate communications channels (e.g., text, chat, social media, internal message boards, etc.)
- Including hotline detail on computer “lock screens” or intranet home pages
- Adding QR codes to posters for easy access to reporting lines when employees are in the office

Beyond advertising the company’s ethics hotline, regulators also want to see that companies are using hotline data to drive their compliance programs. In other words, in addition to responding to hotline complaints, regulators ask whether compliance functions are actually using the underlying hotline data. This could include: issuing guidance around topics that have resulted in significant reporting; targeting markets for auditing where the company has received relevant reports; looking at where reporting is not happening, so compliance can focus its advertising efforts there; and evaluating whether there are trends in reporting (e.g., certain types of reports in certain markets). Hotline reporting contains a wealth of compliance-relevant data that the DOJ expects companies will use to evaluate and improve compliance programs.<sup>30</sup>

Relatedly, the DOJ expects companies to periodically test the hotline’s effectiveness (see Section VI) by, for example, tracking the timeline of a hotline report from start to finish; conducting employee surveys, working groups, or interviews about their view of the reporting hotline, investigations process, and non-retaliation policy; tracking the implementation of remediation; and using exit interview data to evaluate the delta between hotline reporting and exit interview reporting of potential non-compliance.<sup>31</sup>

An ineffective whistleblower program can have significant consequences for a company. Recent enforcement actions clearly show that regulators will be particularly aggressive with companies that receive — but fail to act on — whistleblower reports.<sup>32</sup> For example, in recent enforcement actions the DOJ has called out executives’ — sometimes repeated — failure to investigate or otherwise act on employee red flag reports.

Ineffective whistleblower programs may also lead whistleblowers to seek help elsewhere, such as by going directly to regulators, leading to even costlier investigations and potential enforcement costs. In fiscal year 2021, the SEC received more than 12,200 whistleblower tips — the largest number of whistleblower tips received in a fiscal year, and a nearly 76% increase over 2020 (the second highest number of whistleblower tips in a fiscal year).<sup>33</sup> Also in fiscal year 2021, the SEC awarded approximately \$564 million to 108 whistleblowers.<sup>34</sup> This is both the largest dollar amount and the largest number of individuals awarded in a single fiscal year. The SEC made more whistleblower awards in fiscal year 2021 than in all prior years combined.

This trend is not unique to the US. In 2019, the European Union passed the EU Whistleblower Protection Directive, which requires Member States to establish a set of minimum whistleblower protection standards for certain companies. As such, employees in the EU will have additional reporting avenues external to the company as the Member States’ whistleblower legislation comes online.

The potential to earn whistleblower awards is appealing to employees (and the whistleblower law firms that often help draft whistleblower complaints submitted to the agencies). As a result, companies’ employees should have the option of reporting concerns internally first. Companies should therefore ensure that employees know about the hotline, have faith that reports are being thoroughly investigated and resolved appropriately, and do not fear retaliation.

## Conclusion

This Client Alert provides insights into how companies can think about compliance in light of changing business risks, remote/hybrid workplace challenges, and US regulator expectations. Each company has its own risk profile, risk tolerance, and approach to mitigating compliance, and not every idea presented here will appeal to or work for every company. Latham & Watkins' White Collar Defense & Investigations team — which includes seasoned regulatory practitioners, career defense advocates, and former high-ranking government lawyers — is well positioned to support companies in building a practical compliance program that works for them and aligns with industry best practices and regulator expectations.

---

If you have questions about this Client Alert or would like support in assessing or building your company's compliance program, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

**Joseph Bargnesi**

joseph.bargnesi@lw.com  
+1.202.637.2114  
Washington, D.C.

**Daniel J. Dominguez**

daniel.dominguez@lw.com  
+1.202.637.2225  
Washington, D.C.

**Christopher D. Frey\***

christopher.frey@lw.com  
+1.212.906.1732 / +1.415.395.8279  
New York / San Francisco

**Erin Brown Jones**

erin.brown.jones@lw.com  
+1.202.637.3325  
Washington, D.C.

**Nathan H. Seltzer**

nathan.seltzer@lw.com  
+44.20.7710.1020  
London

**Katherine A. Sawyer**

katherine.sawyer@lw.com  
+1.213.891.8839  
Los Angeles

**Savannah K. Burgoyne**

savannah.burgoyne@lw.com  
+1.202.637.1069  
Washington, D.C.

**Catherine A. Rizzoni**

cat.rizzoni@lw.com  
+1.415.395.8271  
San Francisco

*\* Not admitted to practice in California. Admitted to practice in New York.*

---

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's Client Alerts can be found at [www.lw.com](http://www.lw.com). If you wish to update your contact details or customize the information you receive from Latham, [visit our subscriber page](#).

## Endnotes

<sup>1</sup> [DOJ Announces Policy Changes to "Invigorate" Efforts to Combat Corporate Crime](https://www.lw.com/admin/upload/SiteAttachments/Alert%202905%20final.pdf), LATHAM & WATKINS LLP (Oct. 29, 2021), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202905%20final.pdf>.

<sup>2</sup> THE WHITE HOUSE, UNITED STATES STRATEGY ON COUNTERING CORRUPTION 2 (December 2021) [hereinafter UNITED STATES STRATEGY ON COUNTERING CORRUPTION], <https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf>.

<sup>3</sup> *Transcript: Kenneth Polite Jr. keynote address at Compliance Week 2022*, COMPLIANCE WEEK (May 17, 2022), <https://www.complianceweek.com/regulatory-enforcement/transcript-kenneth-polite-jr-keynote-address-at-compliance-week-2022/31698.article>.

- 
- <sup>4</sup> *Updated DOJ Guidance on Corporate Compliance Programs Emphasizes Technology, Real-Time Compliance Data, and Lessons Learned*, LATHAM & WATKINS LLP (June 4, 2020), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202753.v2.pdf>.
- <sup>5</sup> See U.S. DEP'T OF JUSTICE, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS 13-14 (Updated June 2020) [hereinafter EVALUATION OF CORPORATE COMPLIANCE PROGRAMS], <https://www.justice.gov/criminal-fraud/page/file/937501/download>.
- <sup>6</sup> *Id.* at 12 (“Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities?”).
- <sup>7</sup> EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 12 (“How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers?”).
- <sup>8</sup> *Id.* at 11 (“Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report?”); 12 (“Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of senior management present for these meetings?”).
- <sup>9</sup> EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 12 (“Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same?”).
- <sup>10</sup> *Id.* at 10-11.
- <sup>11</sup> *US Regulators Increase Focus on Corporate Compliance and Its Gatekeepers*, LATHAM & WATKINS LLP (Aug. 1, 2022), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202986.pdf>.
- <sup>12</sup> *Transcript: Kenneth Polite Jr. keynote address at Compliance Week 2022*, COMPLIANCE WEEK (May 17, 2022), <https://www.complianceweek.com/regulatory-enforcement/transcript-kenneth-polite-jr-keynote-address-at-compliance-week-2022/31698.article>.
- <sup>13</sup> *Updated DOJ Guidance on Corporate Compliance Programs Emphasizes Technology, Real-Time Compliance Data, and Lessons Learned*, LATHAM & WATKINS LLP (June 4, 2020), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202753.v2.pdf>.
- <sup>14</sup> See, e.g., Press Release, U.S. Secs. & Exch. Comm'n, SEC Files Multiple Insider Trading Actions Originating from the Market Abuse Unit's Analysis and Detection Center (July 25, 2022), <https://www.sec.gov/news/press-release/2022-129>.
- <sup>15</sup> See, e.g., *Health Care Fraud Unit*, U.S. DEP'T OF JUSTICE, <https://www.justice.gov/criminal-fraud/health-care-fraud-unit>; see also U.S. Dep't of Justice, Fraud Section Year in Review 2017 10 (2017), <https://www.justice.gov/criminal-fraud/file/1026996/download> (announcing the 2017 launch of the Health Care Fraud Unit's Data Analytics Team).
- <sup>16</sup> See, e.g., Alfredo Collosa, *Use of Big Data in Tax Administrations*, INTER-AMERICAN CENTER OF TAX ADMINISTRATIONS (Sep. 1, 2021), <https://www.ciat.org/use-of-big-data-in-tax-administrations/?lang=en>; TRANSPARENCY INTERNATIONAL, OPEN DATA AND THE FIGHT AGAINST CORRUPTION IN BRAZIL (2017) [http://webfoundation.org/docs/2017/04/2017\\_OpenDataBrazil\\_EN-2.pdf](http://webfoundation.org/docs/2017/04/2017_OpenDataBrazil_EN-2.pdf).
- <sup>17</sup> UNITED STATES STRATEGY ON COUNTERING CORRUPTION, *supra* note 2, at 35.
- <sup>18</sup> *Id.*
- <sup>19</sup> *Transcript: Kenneth Polite Jr. keynote address at Compliance Week 2022*, COMPLIANCE WEEK (May 17, 2022), <https://www.complianceweek.com/regulatory-enforcement/transcript-kenneth-polite-jr-keynote-address-at-compliance-week-2022/31698.article>.
- <sup>20</sup> EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 2.
- <sup>21</sup> *Transcript: Kenneth Polite Jr. keynote address at Compliance Week 2022*, COMPLIANCE WEEK (May 17, 2022), <https://www.complianceweek.com/regulatory-enforcement/transcript-kenneth-polite-jr-keynote-address-at-compliance-week-2022/31698.article> (emphasis added).
- <sup>22</sup> “Prosecutors should also assess ... how the company measures the effectiveness of its training curriculum.” EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 5.
- <sup>23</sup> *US Regulators Increase Focus on Corporate Compliance and Its Gatekeepers*, LATHAM & WATKINS LLP (Aug. 1, 2022), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202986.pdf>.
- <sup>24</sup> *Updated DOJ Guidance on Corporate Compliance Programs Emphasizes Technology, Real-Time Compliance Data, and Lessons Learned*, LATHAM & WATKINS LLP (June 4, 2020), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202753.v2.pdf>.
- <sup>25</sup> *Id.*
- <sup>26</sup> EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 10.
- <sup>27</sup> See, e.g., *Prioritizing Corporate Culture: Lessons for Companies from the Major League Baseball Sign-Stealing Investigation*, LATHAM & WATKINS LLP (Jan. 17, 2020), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202579.v5.pdf>.
- <sup>28</sup> LATHAM & WATKINS LLP, *CULTURE – A PRACTICAL FRAMEWORK FOR SUSTAINABLE CHANGE* (3d ed. 2021), <https://www.lw.com/en/insights/culture-framework-sustainable-change>.
- <sup>29</sup> EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 6.
- <sup>30</sup> EVALUATION OF CORPORATE COMPLIANCE PROGRAMS, *supra* note 5, at 6-7.
- <sup>31</sup> *Id.*

---

<sup>32</sup> *Risks of Tuning Out Company Whistleblowers: Ignorance Is Not Bliss*, FORBES (June 15, 2022), <https://www.forbes.com/sites/insider/2022/06/15/risks-of-tuning-out-company-whistleblowers-ignorance-is-not-bliss/?sh=2ae174f16571>.

<sup>33</sup> 2021 ANNUAL REPORT TO CONGRESS: WHISTLEBLOWER PROGRAM, U.S. SEC. & EXCH. COMM'N 2 (2021), <https://www.sec.gov/files/owb-2021-annual-report.pdf>.

<sup>34</sup> *Id.* at 1.