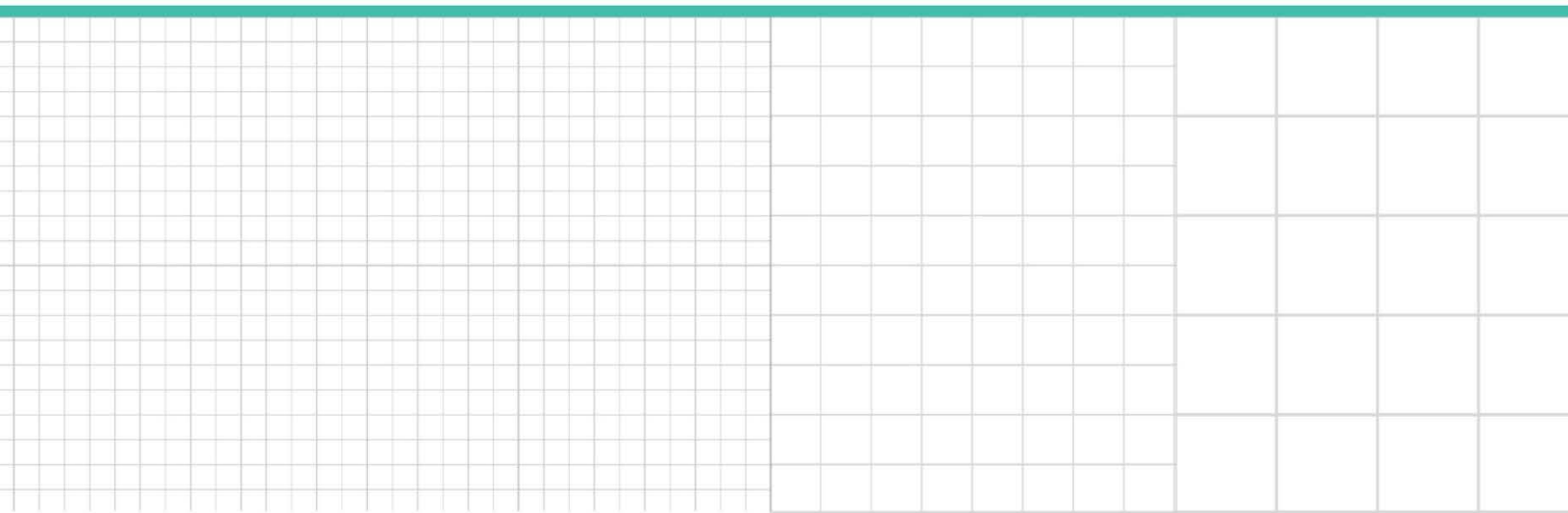


Professional Perspective

DOJ Guidance on Evaluating Corporate Compliance Programs

*Kevin Muhlendorf, Brandon Moss, Madeline Cohen,
and Ashley Bouchez, Wiley*

Reproduced with permission. Published June 2020. Copyright © 2020 The Bureau of National Affairs, Inc.
800.372.1033. For further use, please visit: <http://bna.com/copyright-permission-request/>



DOJ Guidance on Evaluating Corporate Compliance Programs

Contributed by *Kevin Muhlendorf, Brandon Moss, Madeline Cohen, and Ashley Bouchez, Wiley*

In an encouraging development, the Department of Justice Criminal Division announced revisions to its year-old guidance for its prosecutors on how they should evaluate corporate compliance programs. The new guidance refines the various factors against which compliance programs will be measured in the event DOJ is tasked with determining how, and whether, to penalize an entity as part of a criminal investigation and resolution.

The updated guidance largely tracks DOJ's longstanding central tenets of an effective compliance program: programs should be thoughtfully designed, consistently applied, and effective. Though the update is aimed at DOJ's own prosecutors, by focusing on the changes, practitioners can understand DOJ's current areas of interest and incorporate those concepts into existing compliance programs. This roadmap may especially help in higher-risk industries, like health care and government contracts, where compliance challenges often arise.

DOJ prosecutors will be asking companies to corroborate their policies with hard data collected over the life of a program. In particular, DOJ will now ask what a company has done beyond initial due diligence with respect to third-party partners and how it has integrated an acquired entity into its compliance program.

Overall, the guidelines reiterate the value DOJ places on the importance of regularly testing, reviewing, and updating corporate compliance programs to account for evolving risks and circumstances. The guidelines, which first started as a smaller series of questions posed by then-DOJ Fraud Section compliance consultant Hui Chen, were first released in 2017 and last revised in 2019.

The newest iteration, released on June 1, 2020, includes additional information reflecting the importance DOJ places on companies ensuring that compliance programs are dynamic and updated to fit changing circumstances. In releasing the new guidance, Criminal Division head Brian Benczkowski said the revisions were "based on our own experience and important feedback from the business and compliance communities."

The Revisions

At the outset of the revised guidance, DOJ expands on its principle that prosecutors make an "individualized determination in each case," requiring that they consider factors such as "the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program."

The revised introduction also directs prosecutors to evaluate programs not only at the time of the offense, but at the time of any charging decision and resolution—allowing DOJ to give (or not give) credit for remedial measures taken after a violation occurs. The rest of the guidance follows the same structure as the prior iteration, dividing prosecutors' queries into three categories: program design, program application, and program efficacy.

Program Design

The revised guidance asks "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." DOJ's approach includes flexibility for different types of compliance programs, allowing prosecutors to credit risk-based programs if they allot adequate resources to evaluating "high-risk transactions," even if such a program ultimately "fails to prevent an infraction."

In a footnote, DOJ also explains that if foreign law affects how a company designs or implements its program, prosecutors will ask how the company determined the effect of foreign law and how it has attempted to maintain an effective compliance program in light of any legal restrictions.

Emphasizing the importance of evolution in compliance programs, the revised guidance also urges prosecutors to determine whether periodic review of the company's compliance program looks only to "a 'snapshot' in time" or is "based upon continuous access to operational data and information across functions." It also asks whether the company has "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" in the same region or industry.

DOJ also emphasizes the importance of employee access to company compliance policies, procedures, and training. The updated guidance asks if policies and procedures have "been published in a searchable format for easy reference," and whether the company tracks employee access to such policies and procedures.

Companies are expected to provide training to employees commensurate with the company's size, sophistication, and industry. With respect to any training, prosecutors will ask if the company provides "a process by which employees can ask questions arising out of the trainings," and a procedure for educating employees who fail post-training testing. Companies should also evaluate "the extent to which the training has an impact on employee behavior or operations." In addition, DOJ will query whether companies "take measures to test whether employees are aware of" reporting mechanisms such as hotlines and whether they test the effectiveness of reporting mechanisms from "start to finish."

The revised guidance adds nuance to DOJ's scrutiny of third-party practices. Prosecutors will ask if a company has documented "the business rationale" for bringing any third party in a transaction "and the risks posed by third-party partners." They will also determine whether third parties have access to the company's reporting mechanisms. Finally, DOJ will inquire whether the company engages "in risk management of third parties throughout the lifespan of the relationship or primarily during the onboarding process."

DOJ has also refined its guidance with respect to mergers and acquisitions. Companies are expected to not only perform initial due diligence on targets, but also create "a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls." Prosecutors will also ask whether a company has procedures for "conducting post-acquisition audits[] at newly acquired entities." Due diligence at the outset of a transaction is not enough.

Program Application

The revised guidance reiterates DOJ's focus on adequately resourcing compliance programs and personnel. Prosecutors will ask whether employees responsible for implementing a company's program are "empowered to function effectively," stating that, "Even a well-designed compliance program" may not succeed if it is "under-resourced." As stated, DOJ also emphasizes that a robust compliance culture is one promoted "at all levels of the company," including by middle management.

"Data resources and access" are also key to effective program application under the newest guidelines. Prosecutors should determine whether "compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions" and whether "any impediments exist that limit access to relevant sources of data."

Program Efficacy

Few changes were made to the section on program efficacy, but DOJ did add a new question emphasizing the dynamic nature of compliance programs: "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?"

Key Takeaways

DOJ wants companies to be able to demonstrate that compliance programs were intentional, well-reasoned, and dynamic. To prove that to DOJ, companies should focus on four goals.

Data Is Key

Programs that do not include the collection and analysis of data to test and improve the program's structure and implementation will struggle to pass DOJ's scrutiny. For DOJ, a company's use of data indicates that it is well-positioned to identify new risks in a timely manner. Reliance on company-specific data also indicates that the company is focused on crafting a program that fits its specific risk profile and adjusting to new risks as they arise. Considering key data like what policies and procedures employees access most can help companies evolve policies that are both responsive to company needs and likely to be used—not just put on a shelf to gather dust.

Commit Resources

A compliance program is only as good as the resources the company is willing to commit. From executives at the top to employees in the field, DOJ wants to see compliance programs that are thoughtful in how they educate employees, empower compliance officials, and remediate problems when they are uncovered. In considering whether a program meets that threshold, DOJ will carefully scrutinize key indicators like the resources a company has dedicated to its compliance and training functions, and the qualification and seniority of the people tasked with implementing the same.

In some ways, this point of emphasis goes hand in hand with DOJ's focus on data—only companies that have sufficiently invested in compliance will have access to the data needed to identify unique risks and adjust their programs accordingly. Without investing in the tools necessary to generate and collect data, and people to analyze the data, there will be no data to monitor for breaches or consider when evolving the compliance program. While not every company is expected to have a million-dollar compliance program, DOJ will expect that a company's compliance program is appropriately scaled to its relevant risk. In short, investment is important to consider when assessing a company's commitment to compliance.

Documentation of Decisions

Decisions related to compliance issues need to be documented from concept to completion. Not only does documentation allow a company to show DOJ the steps it took in the event of a compliance failure, but the process of compiling the documentation lends itself to a conclusion that the decision was a well-reasoned and considered one. DOJ is clearly signaling that while compliance failures will inevitably happen, if a company can show that the decisions leading up to the failure were intentional and well meaning, and were followed by remedial action, prosecutors should be more willing to issue a declination.

Third-Party Scrutiny

Scrutiny of third parties and acquired entities cannot end at the close of due diligence or onboarding. Companies must continue to assess and address risks posed by third parties throughout their relationship—it is not enough simply to ensure that the third party has a clean bill of health when the company enters the arrangement. Similarly, while quality due diligence is essential, companies should go beyond that and ensure that the acquired entity is successfully integrated into the company's compliance program. Of course, DOJ will also examine whether the company's compliance program was updated post-acquisition to account for any new risks associated with the acquired company, and whether there are adequate provisions for post-acquisition audits.

Conclusion

Even though the updated guidance does not substantially change what DOJ has said for years about the central tenets of an effective compliance program, it does offer important additional details. The vast majority of companies will never have their compliance programs subject to this rigorous analysis by DOJ. However, the factors and questions DOJ has put forth in this guidance create a more sophisticated roadmap for companies to better protect themselves from the sort of failings that could result in criminal, civil, or regulatory scrutiny.

In that sense, the guidance can also bring a degree of comfort to those operating in high-risk industries like health care, government contracts, and financial services, where a compliance issue seems to be more of a “when” than an “if” proposition.

While adherence to the guidelines does not provide a safe harbor if something goes wrong, it can provide a level of comfort that the company will be on the best footing possible to identify risks, address failures, and receive credit for its efforts if called upon to defend what went wrong.