

DOJ makes changes to its corporate compliance guidance

September 26, 2024 | Client Update | 5-minute read

DOJ made changes to its Evaluation of Corporate Compliance Programs, the first since March 2023. The changes focus on the management of technology risk, including the use of artificial intelligence, as well as whistleblower retaliation, data analytics, M&A integration, and how companies handle instances of misconduct beyond those under investigation.

On September 23, 2024, the Department of Justice (DOJ) released a revised version of the Evaluation of Corporate Compliance Programs (ECCP), which is designed to guide prosecutors in evaluating the effectiveness of compliance programs, and is a resource for companies to understand DOJ's compliance expectations. The revisions reflect DOJ's continued efforts to heighten and refine its standards for an effective compliance program, a long-running evolution that now dates back more than a decade.

Notable revisions

Technology risk/artificial intelligence. DOJ officials have made several recent announcements and speeches regarding the risks posed by artificial intelligence, and therefore it is not surprising that the ECCP revisions focus on technology risk. The ECCP questions and considerations now include:

- Whether the company has conducted a risk assessment regarding the use of technology, particularly new and emerging technology such as AI, and whether it has taken appropriate steps to mitigate any risk associated with the use of that technology.
- How is the company curbing any potential negative or unintended consequences resulting from the use of technologies, both in its commercial business and in its compliance program?
- How is the company mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders?
- To the extent that the company uses AI and similar technologies in its business or as part of its compliance program, are controls in place to monitor and ensure its trustworthiness, reliability, and use in compliance with applicable law and the company's code of conduct?
- How is accountability over use of AI monitored and enforced?
- How does the company train its employees on the use of emerging technologies such as AI?

Data access and data analytics. Although the ECCP has long asked whether compliance programs have appropriate access to data, it now asks whether the company is “appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs,” as well as how the “assets, resources, and technology available to compliance and risk management compare to those available elsewhere in the company.” It specifically asks whether there is an “imbalance between the technology and resources used by the company to identify and capture market opportunities and the technology and resources used to detect and mitigate risks.”

Lessons learned and training. Although the ECCP previously asked whether companies were incorporating “lessons learned” into their compliance programs in various ways, it now also asks whether companies are leveraging lessons learned from other companies in similar industries or operating in similar regions into their policy designs and trainings. It also asks whether the company’s trainings are “tailored to the particular needs, interests, and values of relevant employees.”

Anti-retaliation and reporting. The new ECCP added a section of questions on “Commitment to Whistleblower Protection and Anti-Retaliation,” a heightened concern given DOJ’s own new [Whistleblower Pilot Program](#). This section includes whether the company has an anti-retaliation policy, trains employees on internal reporting systems *as well as* external whistleblower programs and regulatory regimes, and disciplines employees who reported internally differently than others involved in misconduct who did not.

M&A integration. As part of a company’s M&A process, the ECCP now includes questions around the integration process, such as whether the company accounts for “migrating or combining critical enterprise resource planning systems,” and the extent to which “compliance and risk management functions play a role in designing and executing the integration strategy.” Along the same lines, the ECCP also now asks whether the company has a process in place “to ensure appropriate compliance oversight of the new Business,” and whether and how the new business is incorporated into the company’s risk assessment activities.

Proven track record. DOJ has also added language around the need for prosecutors to “consider whether the company’s compliance program had a track record of preventing or detecting other instances of misconduct,” which can include an analysis of how the company “responded to other instances of misconduct in addition to how the company addressed reports of potential misconduct and risks over time.”

Key takeaways

- It may sound logical and noncontroversial to say that DOJ will look at a company’s “track record” for detecting and addressing misconduct, but what this really means is that DOJ will be asking companies to present on other instances of misconduct that have occurred at the company beyond those under investigation. This new reality should be a factor considered in any voluntary disclosure analysis.
- It is also interesting that DOJ is now expecting companies to train employees not just on how to report misconduct internally, but also how they can report misconduct to regulators. It seems somewhat puzzling and inconsistent that DOJ is encouraging companies to foster a speak-up culture, but also requiring training on external whistleblower programs. Companies should consider carefully how to respond to this change in the ECCP.
- DOJ established earlier this year its “Justice AI Initiative,” and as part of that announced that the ECCP would be revised to include questions around the use of AI. So this addition was expected. More broadly, DOJ is now squarely focusing companies on addressing risks arising from the use of technologies.
- The additions regarding resources devoted to compliance and the use of data analytics as part of a compliance program are also not surprising given that DOJ officials have been making similar statements in speeches. That said, it is now clearly something DOJ expects companies to be thinking about and companies should work through the questions, even in the face of potential inherent challenges in using data analytics as part of their compliance programs.
- Finally, this is yet another reminder of how much DOJ is now prioritizing a company’s commitment to compliance. The DOJ is again making clear that it will go beyond requiring comprehensive policies and training and will examine how effectively a compliance program is implemented in practice. Companies should consider how best to prepare for this sort of searching inquiry.

Linked [here](#) is a redline of the new ECCP against the prior version from March 2023.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres

+1 212 450 4724
greg.andres@davispolk.com

Sidney Bashago

+1 212 450 4826
sidney.bashago@davispolk.com

Martine M. Beamon

+1 212 450 4262
martine.beamon@davispolk.com

Robert A. Cohen

+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin

+1 212 450 4059
james.haldin@davispolk.com

Daniel S. Kahn

+1 202 962 7140
daniel.kahn@davispolk.com

Tatiana R. Martins

+1 212 450 4085
tatiana.martins@davispolk.com

Fiona R. Moran

+1 202 962 7137
fiona.moran@davispolk.com

Paul J. Nathanson

+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.