

DOJ Updates the Evaluation of Corporate Compliance Program Memorandum, Emphasizing Emerging Technologies, Data Analytics, and Whistleblower Protections

by Caitlin L.D. Hull, Nicole Engisch, Seth Goertz, Alex Hontos, and Andrew Stone

On September 23, 2024, the U.S. Department of Justice (“DOJ”) released updates to its Evaluation of Corporate Compliance Programs policy (the “Updated ECCP”),^[1] building upon the March 2023 updates.^[2] Since 2017, DOJ has offered prosecutors various versions of the ECCP as a framework for evaluating the effectiveness of a company’s compliance program. The three “fundamental questions” of a compliance program evaluation—that is, whether the corporation’s compliance program is well designed, adequately resourced and empowered to function effectively, and works in practice—remain unchanged. However, the Updated ECCP underscores DOJ’s evolving focus on emerging technologies and data-driven compliance—including artificial intelligence (“AI”)—and whistleblower protections, along with an increased emphasis on post-acquisition integration and routine risk assessments. Understanding these changes and their implications is essential to maintaining an effective compliance program that can withstand DOJ scrutiny.

1. Key Enhancements

a. Emerging Technologies and Data Analytics

As technology continues to transform industries, its implications for compliance are multifaceted. Indeed, the most substantive revisions to the ECCP focus on emerging technologies, such as AI, and the use of data and technology as part of a company’s compliance program and controls.

First, the Updated ECCP focuses extensively on technology risks. This reveals DOJ’s ongoing concern that companies use technology responsibly and effectively mitigate the risks of misuse of technology. In particular, DOJ expects companies to navigate the complex landscape of AI—both its potential risks and benefits—while also ensuring that compliance programs are robust enough to keep pace with cyber criminals. The revised guidance sets forth ten questions that companies should use when assessing and

Related People

- Caitlin L.D. Hull
- Nicole Engisch
- Seth Goertz
- Alex Hontos
- Andrew Stone

Related Capabilities

- Government Enforcement & Corporate Investigations
- Corporate Governance & Compliance

managing these risks:

1. How does the company assess the potential impact of new technologies, such as AI, on its ability to comply with criminal laws?
2. Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management strategies?
3. What is the company's approach to governance regarding the use of new technologies, such as AI, in its commercial business and in its compliance program?
4. 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?
5. How is the company mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders?
6. 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 that these technologies are trustworthy, reliable, and comply with applicable law and the company's code of conduct?
7. Are controls in place to ensure that the technology is used only for its intended purposes?
8. What baseline of human decision-making is used to assess AI and similar technologies?
9. How is accountability over use of AI and similar technologies monitored and enforced?
10. How does the company train its employees on the use of emerging technologies such as AI?

Second, the Updated ECCP stresses the importance of ongoing risk assessments tailored to the company's actual practices, highlighting the need for a company to identify, assess, and prioritize emerging risks—like AI—as its business evolves.

Lastly, DOJ has now made clear that it expects data analytics to be a key part of effective compliance. The Updated ECCP encourages companies to leverage data analytic tools to detect and prevent misconduct, including leveraging its data to gain insights into the effectiveness of its compliance program. To this end, the Updated ECCP also highlights a renewed and explicit focus on whether compliance programs are adequately and *proportionately* resourced when compared to resources utilized for commercial purposes. Stated differently, DOJ has suggested that it will look with disfavor upon a company where 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.”

b. Confidential Reporting Structure and Investigation Process

The Updated ECCP also reinforces the importance of a well-designed confidential reporting structure and internal investigation process as a key part of a corporate compliance program. With that in mind, the Updated ECCP suggests three key enhancements and considerations:

1. The company should not only have an anonymous reporting mechanism for employees (e.g., an anonymous hotline), but the company should actively “encourage and incentivize reporting” and ensure there is not a “chilling effect” for employees who use the reporting mechanism.
2. The company should actively reduce the fear of and prevent retaliation through, for example, strong anti-retaliation policies and periodic training on non-retaliation and whistleblower reporting procedures.
3. The company should “assess employees’ willingness to report misconduct.”

Overall, these enhancements are consistent with recent amendments to DOJ’s Corporate Enforcement and Voluntary Self-Disclosure Policy and newly-launched pilot whistleblower program, which aims to incentivize both individuals to report corporate criminal wrongdoing *and* self-disclosure of corporate wrongdoing by corporations even prior to DOJ involvement.^[3]

c. Integration Processes and Post-Transaction Compliance

In the mergers and acquisition context, the Updated ECCP also reinforces the importance of pre- and post-acquisition due diligence and integration of post-transaction compliance programs. In short, DOJ has clarified that it not only expects acquirers to have strong compliance diligence on the front end of an acquisition, but acquirers should also have a method of appropriately overseeing and affirmatively incorporating the acquired business into the overall risk profile, such as by conducting post-acquisition audits.

d. Routine Risk Assessments

Woven throughout the Updated ECCP is also a renewed focus on companies completing routine risk assessments to ensure that they proactively identify emerging risks and adjust their compliance programs appropriately. While this concept is not new—and, indeed, has long been a cornerstone of an effective compliance program—the Updated ECCP reiterates the need for companies to have a process that continually assesses risks as they arise. Each company should therefore review its “process for identifying and managing emerging internal and external risks that could potentially impact the company’s ability to comply with the law, including risks related to the use of new technologies,” with an eye toward being proactive rather than reactive.

2. Key Takeaways and Action Items

With the Updated ECCP in hand, compliance and legal teams should take the following steps to ensure that their programs continue to bear the hallmarks of an “effective” compliance program:

- **Review Compliance Programs:** Review compliance policies and procedures for comprehensiveness and proportionality, especially as it relates to AI and technology. For many companies, this may involve bringing new groups (e.g., technology, privacy, or security) into the compliance conversation to ensure that the company has a fulsome understanding of both its risk profile and its current practices.
- **Update Policies and Procedures:** Review and revise any policies affected by the new guidance, including, for example, strengthening training and communications regarding whistleblower retaliation protections and authorized use of AI.
- **Leverage Technology:** Assess current data analytics capabilities and ensure the company can implement data analytics to support compliance efforts, including to detect misconduct, measure compliance effectiveness, and inform program improvements.
- **Document Compliance Efforts:** Maintain thorough records of compliance activities, including risk assessments, training, and audits.
- **Ensure Appropriate Responses to Misconduct:** Conduct prompt, credible investigations of complaints about non-compliance and misconduct and, where appropriate, evaluate whether to provide timely voluntary self-disclosure to DOJ.

By understanding these updates and implementing these key takeaways, companies can strengthen their compliance programs and show a commitment to ethical and lawful business practices that may in turn minimize DOJ’s scrutiny or penalties in the event of a whistleblower complaint or independent DOJ investigation.

[1] The [Updated ECCP](#) is available. For the press release announcing the updated ECCP, see [Office of Public Affairs | Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute | United States Department of Justice](#).

[2] See [Department of Justice Announces First-Ever Pilot Program on Compensation Incentives and Clawbacks, Revisions to Corporate Guidance Regarding Electronic Communications, and Resource Commitments for Corporate Compliance with Sanctions and Export Control Laws | News & Resources | Dorsey](#)

[3] For a review of DOJ’s recently-implemented corporate whistleblower program, see [DOJ’s New Whistleblower Program Incentivizes Individuals and Corporations to Disclose Wrongdoing | News & Resources | Dorsey](#)