



Key Updates to the DOJ's Evaluation of Corporate Compliance Programs

Posted by Andrew M. Good, Avia M. Dunn, and Zaneta Wykowska, Skadden, Arps, Slate, Meagher & Flom LLP, on Monday, October 7, 2024

Editor's note: Andrew M. Good and Avia M. Dunn are Partners, and Zaneta Wykowska is an Associate at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on a Skadden memorandum by Mr. Good, Ms. Dunn, Ms. Wykowska, Ryan D. Junck, and William E. Ridgway.

On September 23, 2024, the U.S. Department of Justice (DOJ) updated its [Evaluation of Corporate Compliance Programs](#) (ECCP) guidance. First published in 2017, the ECCP sets out factors that DOJ Criminal Division prosecutors will consider when evaluating the compliance program of a company facing a criminal enforcement action. While primarily intended for prosecutors, the ECCP also serves as a valuable resource for companies to assess how their programs might be judged by the DOJ. A company with an effective compliance program is more likely to receive a favorable resolution in an enforcement action, including reduced monetary penalties and less burdensome ongoing compliance obligations, as part of the resolution terms.

Several revisions to the ECCP since its inception highlight the DOJ's focus on understanding the rationale behind the program's design, evolution over time and functionality in addressing the relevant company's risk profile.

Companies should note the following key additions introduced in the latest ECCP update:

1. **Risks Associated With New and Emerging Technology:** The updated ECCP includes new criteria to evaluate how companies are assessing and managing risks related to the use of new technology such as artificial intelligence (AI) in their commercial operations and compliance programs.
2. **Incentivizing and Protecting Whistleblowers:** The updated ECCP bolsters the DOJ's expectations that corporations should actively promote internal whistleblowing and safeguard individuals who report misconduct. Going forward, the DOJ will evaluate whether companies have adequate policies and training to encourage whistleblowing and prevent retaliation, as well as how companies treat employees who report misconduct.
3. **Access to Data and Resources for Compliance Functions:** The revisions emphasize the DOJ's stance that the effective operation of a compliance program requires a compliance function that is sufficiently resourced and funded and has access to the data and technology necessary to detect and mitigate risks. DOJ prosecutors will evaluate

whether compliance functions (i) have timely access to data and (ii) appropriately leverage data analytics tools to create efficiencies in the compliance program and track its effectiveness.

4. **Incorporating Lessons Learned:** The updated ECCP also emphasizes that compliance programs and employee training should evolve based on lessons learned from both the company's own prior issues and from issues at other companies in related industries and geographies.
5. **Post-Transaction Compliance Integration:** The latest revisions underscore the importance of compliance function involvement in M&A activity, in particular post-transaction integration.

Together, these updates provide a clearer framework for companies to ensure their compliance programs are robust and aligned with DOJ expectations.

Risks Associated With New and Emerging Technology

In March 2024, Deputy Attorney General Lisa Monaco warned that individuals and companies could face increased penalties for deliberately misusing AI to commit white-collar crimes and directed the DOJ Criminal Division to incorporate assessment of disruptive technology risks into the ECCP. [1] Accordingly, the ECCP now instructs prosecutors to evaluate how companies measure and manage risks of new technology, including AI, both in their business operations and in their compliance programs.

Prosecutors evaluating the design of a company's compliance program will consider:

- Whether the company has assessed the risks associated with new and emerging technology, such as AI, including on the company's ability to comply with criminal laws, and taken appropriate steps to mitigate any risk associated with use of that technology in its commercial business and compliance program.
- Whether the company has implemented and updated policies and procedures to address emerging risks, including those associated with the use of new technologies.
- The company's approach to governance regarding the use of new technologies such as AI in its commercial business and compliance program and how the use of AI is monitored and enforced.
- Controls in place to monitor the reliability of and potential negative or unintended consequences resulting from the use of technologies in both commercial business and compliance programs.

- The company's approach to training employees on the use of emerging technologies such as AI.

To ensure they meet DOJ expectations regarding AI and other emerging technologies, companies must first understand how those technologies are deployed and used within their operations, assess the resulting unique risk profile, and establish policies and procedures to mitigate these emerging risks. Companies are expected to maintain a rigorous framework to manage emerging technology risks, and to review it periodically to ensure proper implementation and monitoring. (See our article in summer 2024 edition of The Informed Board, "[AI Safety: The Role of the Board in Assessing and Managing AI Risk](#).")

Incentivizing and Protecting Whistleblowers

In the past year, the DOJ has intensified its focus on corporate whistleblowing as a critical tool for identifying and addressing corporate misconduct. In April 2024, the DOJ [launched its Pilot Program on Voluntary Self-Disclosure for Individuals](#) to encourage individuals to self-disclose misconduct involving corporations. Then, in August 2024, the DOJ Criminal Division [launched the Corporate Whistleblower Awards Pilot Program](#). The DOJ's focus on whistleblowing is further reflected in its updates to the ECCP, which highlight the importance of maintaining effective mechanisms for the confidential reporting of allegations of misconduct and instructs prosecutors to review companies' policies, training and treatment of employees who report misconduct.

The updated ECCP directs prosecutors to evaluate:

- Whether the company encourages and incentivizes reporting of potential misconduct, or uses practices that could chill such reporting.
- The adequacy of the company's policies and training relating to anti-retaliation and whistleblower protection.
- The treatment of employees involved in misconduct who report the misconduct compared to the treatment of others involved in misconduct who do not report it.

The DOJ's recent initiatives and ECCP updates spotlight a clear trend toward leveraging whistleblowing as a key mechanism for uncovering corporate misconduct. Companies should review and strengthen their whistleblower policies to encourage reporting of misconduct and implement vigorous protections for whistleblowers.

Access to Data and Resources for Compliance Personnel

The updated ECCP also reflects the DOJ's continued emphasis on resourcing and data access for the proper functioning of a compliance program. The updates highlight the importance of providing

compliance functions with access to data, including leveraging data to identify misconduct and assess the effectiveness of the compliance program.

The updated ECCP directs prosecutors to ask additional questions about the assets, resources and technology available to compliance personnel, including:

- Whether the company has a mechanism to measure the value of investments in compliance and risk management.
- The company's use of data analytics tools to create efficiencies in compliance operations and to measure the effectiveness of the company's compliance program.
- The company's approach to managing the quality of its data sources and data analytics models.
- Whether the company dedicates the same resources and technology to gathering and leveraging data for compliance purposes as it does for commercial purposes.

The DOJ recognizes that effective compliance programs depend greatly on the ability to use and interpret data. The DOJ will acknowledge and credit companies that utilize data analytics, considering their use of these tools as a positive factor when evaluating the effectiveness of their compliance efforts. Companies should investigate the availability of technology-driven compliance tools that can be integrated with their existing data sources both to identify potential misconduct and to assess the performance of their compliance programs. By adopting advanced technological solutions, companies can position themselves advantageously during regulatory investigations.

Incorporating Lessons Learned

Announcing the ECCP updates, Principal Deputy Assistant Attorney General Nicole Argentieri noted that "companies should be learning lessons from both the company's own prior misconduct and from issues at other companies to update their compliance programs and train employees." [2] Accordingly, the revised ECCP features additional questions intended to assess how a company's compliance program has evolved and improved based on recognized issues internally and in the market.

The updated ECCP instructs prosecutors to consider:

- Whether policies, procedures and controls have been updated to account for risks discovered through misconduct or other problems with the company's compliance program.
- Whether the company has a process for tracking and incorporating lessons learned from the company's prior issues or from those of other companies in the same industry and/or geographical region into its risk assessment.

- Whether the company’s training addresses (i) risks in areas where misconduct has occurred and (ii) areas for improvement gleaned from prior compliance incidents.

Given the recent updates to the ECCP, companies should update their compliance policies and controls based on an evaluation of identified issues and benchmarking assessment against similar organizations. By doing so, companies can ensure their compliance programs are tailored to specific risks and effectively address the most pertinent threats.

Post-Transaction Compliance Integration

The latest ECCP revisions stress the importance of the compliance function having a prominent “seat at the table” in evaluating and de-risking M&A activity. (See our October 5, 2023, client alert [“DOJ Announces Safe Harbor Policy for Voluntary Self-Disclosures Related to Mergers & Acquisitions.”](#)) The updated ECCP instructs prosecutors to consider:

- The company’s approach to, and the role of compliance and risk management functions in, the design and execution of post-transaction integration strategy.
- The company’s process for (i) implementing and/or integrating a compliance program post-transaction, (ii) incorporating the new business into the company’s risk assessment activities and (iii) compliance oversight of the new business.
- Whether post-acquisition audits are conducted at newly acquired entities.

Companies should examine their post-transaction integration procedures to ensure newly acquired businesses are subject to appropriate scrutiny and effectively incorporated into compliance programs.

Conclusion

Companies should consider reviewing their compliance programs in response to the additional factors incorporated into the ECCP. This review should assess whether the company has sufficient measures to address risks associated with AI and other emerging technologies, whether robust mechanisms are in place to promote whistleblowing within the organization and how to conduct adequate post-transaction compliance oversight of newly acquired businesses. The DOJ is also intensifying its focus on the compliance function’s access to comprehensive organizational data. The agency expects companies to utilize this information to continuously update and refine their compliance programs, drawing on lessons learned from both internal and external issues.

¹See Deputy Attorney General Lisa Monaco, [Keynote Remarks at the American Bar Association’s 39th National Institute on White Collar Crime](#) (March 7, 2024).[\(go back\)](#)

²See Principal Deputy Assistant Attorney General Nicole M. Argentieri, [Address at Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute](#) (Nov. 23, 2024).([go back](#))