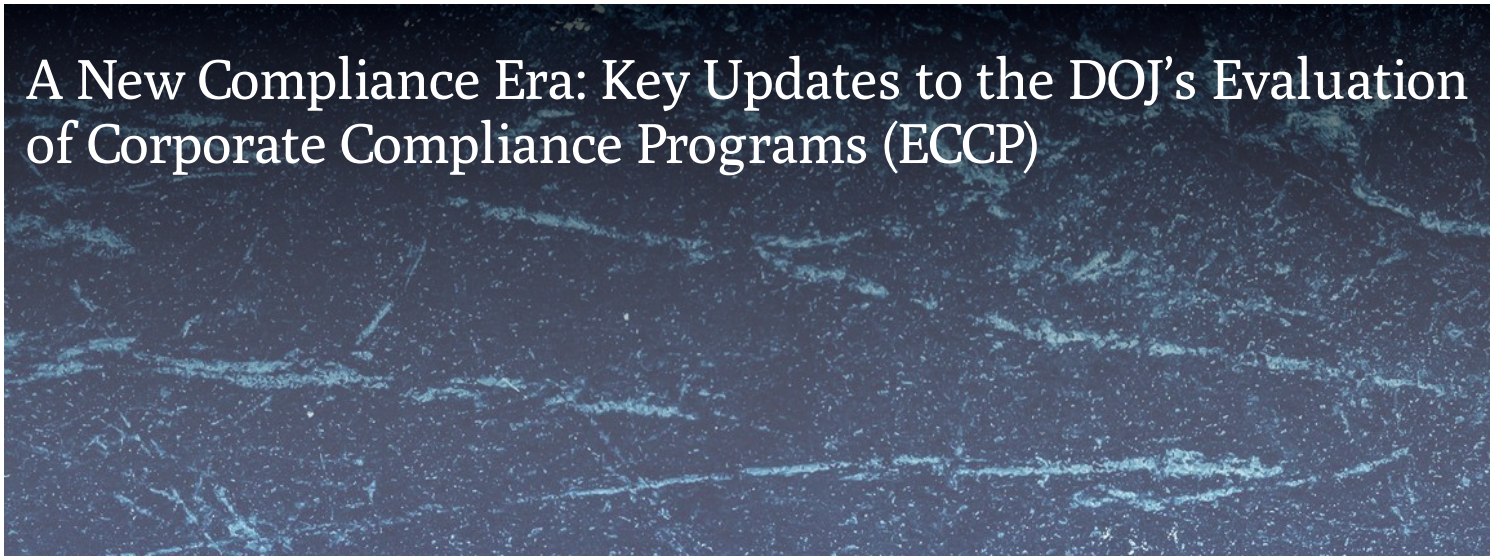
WINSTON & STRAWN LLP

BLOG

A New Compliance Era: Key Updates to the DOJ's Evaluation of Corporate Compliance Programs (ECCP)



SEPTEMBER 26, 2024

KEY TAKEAWAYS

The U.S. Department of Justice (DOJ) recently updated its Evaluation of Corporate Compliance Programs (ECCP) to reflect emerging challenges in corporate compliance. In the September 2024 update, the DOJ introduced three significant changes:

- **Artificial Intelligence Risk Mitigation**: The ECCP now emphasizes the need for companies to address risks and mitigation efforts associated with the use and misuse of artificial intelligence (AI).
- **Whistleblower Protection and Encouragement**: DOJ will place increased focus on how companies encourage or discourage whistleblowing, with specific guidance on evaluating whistleblower programs and whether the company's complaint-handling process includes proactive measures to create an environment that protects whistleblowers from retaliation.
- **Access to Company Data for Compliance**: Prosecutors must now consider whether compliance programs have sufficient access to necessary company data to proactively identify misconduct or deficiencies, and effectively monitor the company's policies, controls, and transactions.

These changes aim to foster stronger corporate compliance frameworks, encouraging a culture of transparency and accountability while addressing modern technological challenges.

BACKGROUND ON THE ECCP

The ECCP serves as a vital tool for federal prosecutors to assess a company's compliance program during investigations and prosecutions. First introduced in 2019, the ECCP provides prosecutors and companies a framework for evaluating compliance programs based on a set of qualitative and quantitative criteria. It draws from various sources, including existing legal standards, industry best practices, and insights gained from the DOJ's own experiences. The full ECCP is available at: https://www.justice.gov/criminal/criminal-fraud/page/file/937501.

On September 23, 2024, the Principal Deputy Assistant Attorney General for the Criminal Division (PDAAG), Nicole Argentieri, announced significant additions to the ECCP, reflecting the evolving landscape of corporate governance,

technological advancements, and the increasing scrutiny on ethical conduct in business operations. The updated ECCP offers more precise guidance for prosecutors evaluating compliance programs, especially concerning AI, whistleblower protections, and data access. As such, the ECCP is an invaluable resource for companies striving to implement and sustain effective compliance programs.

UPDATE #1: ARTIFICIAL INTELLIGENCE RISK MITIGATION

In March 2024, the DOJ indicated its intention to focus on the risks associated with artificial intelligence in corporate compliance evaluations, a concern that DOJ now integrated into the ECCP. In the PDAAG's own words speaking at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute, "prosecutors will consider the technology that a company and its employees use to conduct business, whether the company has conducted a risk assessment of the use of that technology, and whether the company has taken appropriate steps to mitigate any risk associated with the use of that technology. For example, prosecutors will consider whether the company is vulnerable to criminal schemes enabled by new technology, such as false approvals and documentation generated by AI."[1] Prosecutors will examine these aspects, among others, of a company's compliance program:

- **Technology Utilization**: What types of AI technologies does the company employ in its operations? How are these technologies integrated into business processes? Do controls exist to ensure that the technology is used only for its intended purposes? What baseline of human decision-making is used to assess AI?
- **Risk Assessments**: Has the company conducted thorough risk assessments to identify potential misuse of AI, both internally and externally? This includes evaluating how AI might inadvertently facilitate criminal behavior, such as fraud or data breaches, as well as considering external threats that could exploit AI technologies to harm the organization.
- **Mitigation Strategies**: What steps has the company taken to mitigate risks associated with AI, including both internal and external threats? This could involve establishing policies, implementing training programs, and developing oversight mechanisms aimed at preventing and addressing misuse, as well as safeguarding against potential exploitation by outside threats.

This update is significant because it incorporates multiple criteria focused on artificial intelligence integration. Now, companies must not only ensure compliance with existing laws but also anticipate and prepare for new forms of risk that may emerge from rapidly advancing technologies. Prosecutors will expect robust policies and procedures aimed at mitigating AI-related vulnerabilities, placing an onus on companies to proactively manage these risks.

The updates to DOJ's EECP came in response to a directive from Deputy Attorney General Lisa Monaco, who in February warned of stiffer sentences for criminals who rely on the generative technology to advance their misconduct as part of a broader focus on combating AI abuse.

UPDATE #2: WHISTLEBLOWER ENCOURAGEMENT AND AWARDS PROGRAM

Whistleblower programs play a critical role in promoting ethical behavior within corporations by providing a secure channel for employees to report misconduct. Historically, whistleblower protections have been a cornerstone of regulatory compliance, yet the effectiveness of these programs often depends on how employees perceive them. The DOJ's Whistleblower Awards Pilot Program, announced in August 2024, incentivizes employees to report violations of federal law by offering financial rewards for credible information that leads to successful enforcement actions. Suzanne Jaffe Bloom, Co-Chair of Winston's Government Investigations, Enforcement, and Compliance practice, discusses the Corporate Whistleblower Pilot Program, including the kinds of enforcement actions it rewards, in Winston's August 2024 client alert. This initiative not only strengthens enforcement efforts but also promotes a culture of transparency and accountability within organizations by reassuring potential whistleblowers that their contributions will be valued and protected from retaliation. As of August 1, 2024, whistleblowers can now submit original information directly to DOJ's Criminal Division at: www.justice.gov/CorporateWhistleblower.

The updated ECCP places a renewed emphasis on the evaluation of whistleblower programs. The PDAAG stated that DOJ will now focus on whether "companies are encouraging employees to speak up and report misconduct or whether companies employ practices that chill reporting" and directs prosecutors to "closely consider the

company's commitment to whistleblower protection and anti-retaliation," including its policies and training.[2] Key questions for prosecutors now include:

- **Awareness and Accessibility**: Do employees know how to report suspected misconduct? Are reporting channels easily accessible and clearly communicated to all employees?
- **Fear of Retaliation**: Are employees confident that they can report concerns without fear of retaliation? What measures are in place to protect whistleblowers from potential backlash?

The DOJ's updates aim to ensure that compliance programs not only facilitate reporting but also create an environment where employees feel safe and empowered to speak up. This shift recognizes that the effectiveness of compliance programs hinges on employee engagement and the cultural dynamics within an organization.

UPDATE #3: COMPLIANCE PROGRAM SELF-ASSESSMENT AND ACCESS TO DATA

Before the latest changes, the focus of compliance program self-assessment often centered on procedural adherence and external audits. However, the updated ECCP introduces a more introspective approach—one that asks prosecutors to now consider "whether compliance personnel have adequate access to relevant data sources and the assets, resources, and technology that are available to compliance and risk management personnel."[3] This change emphasizes several critical factors:

- **Data Accessibility**: Do compliance officers have access to the necessary data to evaluate the effectiveness of the compliance program? This includes financial data, operational metrics, and information regarding past compliance failures.
- **Resource Allocation**: Are adequate resources allocated to compliance efforts? The PDAAG's comments suggest a balancing test, assessing whether companies invest commensurate resources in compliance relative to their business operations.
- **Continuous Improvement**: Companies must now engage in self-assessment as a means of continuous improvement. This means not only identifying past compliance issues but also proactively analyzing trends and risks that may affect future compliance efforts.

The DOJ's renewed focus on data access and self-assessment marks a shift toward a more dynamic and responsive compliance culture. The updated guidance encourages companies to take ownership of their compliance programs, fostering an environment of continuous learning and adaptation.

IMPLICATIONS FOR YOUR COMPLIANCE PROGRAM

The DOJ's updates to the ECCP signal a broader shift in how it evaluates and prioritizes corporate compliance. These changes present both challenges and opportunities.

1. Emphasis on Proactive Compliance

The incorporation of AI considerations necessitates a proactive approach to risk management. Companies must now invest in understanding the implications of emerging technologies on their operations and compliance frameworks. This means engaging in thorough risk assessments and developing policies that address these risks comprehensively.

2. Culture of Reporting

With increased scrutiny on whistleblower programs, companies should evaluate and enhance their organizations' reporting mechanisms. Creating a culture that encourages reporting requires not only robust policies but also training and communication strategies that emphasize the importance of ethical behavior.

3. Data-Driven Compliance Strategies

As access to data becomes a focal point in compliance evaluations, companies must prioritize the integration of data analytics into their compliance programs. This involves ensuring that compliance teams have the necessary tools

and access to data that inform decision-making and risk assessments.

4. Legal Implications and Risk Management

The updated ECCP highlights the potential legal implications for companies that fail to adapt to these new guidelines. Prosecutors will have clearer frameworks for evaluating compliance failures, which may impact enforcement actions and penalties. As such, corporate attorneys should be vigilant in ensuring that their organizations align with the revised standards.

CONCLUSION

The DOJ's latest updates to the ECCP mark a significant evolution in the landscape of corporate compliance. By focusing on AI risk management, whistleblower protections, and data access, the DOJ is encouraging companies to adopt a more integrated and proactive approach to compliance. These changes present a crucial opportunity to enhance compliance programs, strengthen ethical culture, and mitigate risks in an increasingly complex corporate environment. As DOJ applies the updated ECCP guidelines, companies should adapt swiftly, ensuring that they not only meet regulatory expectations but also foster a culture of integrity and accountability.

For more information or assistance evaluating your company's compliance program or policies, please contact your Winston relationship partner, or Richard Weber, David Kolansky, or Josh Roth.

---

[1] *Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute*, Dep't of Just. (Sept. 23, 2024), https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society

[2] *Id.*

[3] *Id.*

7 Min Read

Authors

Richard Weber

David A. Kolansky

Josh Roth

Related Topics

Compliance

Artificial Intelligence (AI)

Evaluation of Corporate Compliance Programs (ECCP)

Related Capabilities

Government Investigations, Enforcement & Compliance

Related Professionals

Richard Weber

David A. Kolansky

Josh Roth

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.