AI and Corporate Compliance: Best Practices for Addressing the DOJ's Expectations for AI Risk Management

March 2, 2026 Dina Blikshteyn, Tim Newman, Neil Issar

PRACTICES AI and Deep Learning, Criminal Investigations and Defense, White Collar and Investigations

In September 2024, the Criminal Division of the Department of Justice (DOJ) issued a significant update to its Evaluation of Corporate Compliance Programs (ECCP) policy document, introducing detailed guidance on the risks associated with artificial intelligence (AI). With this update and in light of recent enforcement activity, it is clear the DOJ views AI as presenting novel compliance challenges that companies must proactively address. Businesses seeking to maintain effective compliance programs must demonstrate thoughtful governance over both AI development and deployment. And the time for action is now — before noncompliance or wrongdoing occurs and prosecutors look to the ECCP's guidance to make investigative and enforcement decisions.

I. The DOJ's Focus on AI Use and Risks

First published in February 2017, the ECCP is the roadmap the DOJ's prosecutors use to evaluate companies' compliance programs in corporate criminal matters, including the questions prosecutors ask when structuring investigations, making charging decisions, determining appropriate penalties and negotiating resolutions. Even though corporate misconduct has become less of a focus under the current administration, the ECCP remains in effect as a guide for the government and companies alike to assess the effectiveness of a compliance program.

The ECCP is organized around three fundamental questions:

1. Is the compliance program well-designed?
2. Is the program being applied earnestly and in good faith?
3. Does the compliance program work in practice?

To assist prosecutors in answering these questions, the ECCP lists non-exclusive questions and considerations relevant to evaluating corporate compliance. The starting point for the first fundamental question (whether a compliance program is well-designed) is a company's assessment of risks. In September 2024, the DOJ revised the ECCP such that prosecutors now evaluate whether a company's risk assessment includes safeguards to mitigate the risks associated with the use and misuse of emerging technologies such as AI.[1] Specifically, prosecutors ask:

- How does the company assess the potential impact of new technologies, such as AI, on its ability to comply with criminal laws?
- Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk-management strategies?
- What is the company's approach to governance regarding the use of AI in its commercial business and in its compliance program?
- How is the company curbing any potential negative or unintended consequences resulting from the use of AI, 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?
- Are controls in place to monitor and ensure the AI's trustworthiness, reliability, and compliance with applicable law and the company's code of conduct?
- Do controls exist to ensure that AI is used only for its intended purposes?
- What baseline of human decision-making is used to assess AI?
- 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?

For the third fundamental question (whether the compliance program works in practice), prosecutors look at programs' capacity to improve and evolve. After the September 2024 revisions, prosecutors ask:

- If the company is using AI in its commercial operations or compliance program, is the company monitoring and testing AI so that it can evaluate whether it is functioning as intended and consistent with the company's code of conduct?
- How quickly can the company detect and correct decisions made by AI or other new technologies that are inconsistent with the company's values?

In addition to updating the ECCP to include AI-specific questions, the DOJ has also taken aggressive actions against companies that used AI irresponsibly in recent years. For example, the DOJ has opened investigations, brought enforcement actions, and filed statements of interest in lawsuits against companies using AI to allegedly violate the Fair Housing Act and federal antitrust laws. In these cases, the agency has taken the position that housing providers screening rental applicants using algorithms can still be discrimination,[2] and competitors setting prices using AI or pricing algorithms can still be price fixing.[3] Similarly, the Securities and Exchange Commission and Federal Trade Commission have brought enforcement actions against companies making false, misleading and/or deceptive statements about their use of AI.

II. Best Practices for Building an AI-Aware Compliance Program

The ECCP's AI-specific questions make it clear the DOJ expects companies to weave AI governance into their overall risk-management architecture, affirmatively analyze how AI development and deployment might create or exacerbate compliance vulnerabilities, and ensure adequate oversight of any AI-powered tools — whether those tools are used in the companies' revenue-generating activities, compliance functions or both. Companies must also have mechanisms to identify and address both the unintended consequences of good-faith AI use and the risk of AI misuse.

Given these expectations, companies should take concrete steps to enhance their compliance programs to address AI-related risks, including:

- Comprehensive AI risk assessment. Companies should identify precisely where and how AI is being used (e.g., customer-facing applications, internal operations and compliance functions). This includes both approved AI use and "shadow AI," in which employees are using unapproved tools without the company's knowledge. For each instance of AI development and deployment, organizations should evaluate the risks and incorporate them into existing risk-management frameworks.
- Clear policies governing AI use. Company policies and procedures should address acceptable uses of AI tools, required approvals for new AI development and deployments,

data-governance requirements for AI systems, documentation standards and prohibited uses that might create compliance risks. In addition, companies should effectively communicate new policies and policy updates to employees and incorporate them into training.
- Controls to ensure AI trustworthiness and reliability. Companies should have controls such as regular testing and validation protocols, ongoing monitoring of AI outputs for accuracy and consistency, mechanisms to detect bias, drift, or degradation in AI performance, and audit trails that preserve human accountability in AI-assisted decisions.
- Preparation for AI-related misconduct. Companies should identify how employees or third parties might misuse AI, implement technical controls to prevent unauthorized AI development or use, and establish investigation protocols for AI-related incidents. Companies should also consider how AI might be used to facilitate or conceal misconduct and implement detection capabilities accordingly.

Many companies leverage established AI governance frameworks, such as the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF) and the ISO/IEC 42001 standard, to guide their compliance efforts. The AI RMF provides flexible, practical guidance for AI risk management, while the ISO 42001 is a certifiable management-system standard with formal requirements. Companies may use both frameworks in complementary fashion, depending on their operational needs. The frameworks may also satisfy the good-faith requirement for AI compliance during an investigation involving ECCP questions.

III. Conclusion

AI poses distinctive challenges for corporate compliance. Companies that ignore these risks may find themselves disadvantaged in enforcement scenarios, unable to demonstrate the thoughtful governance that prosecutors expect. By preemptively conducting thorough AI risk assessments, implementing robust controls, training employees appropriately and drawing on existing AI governance frameworks, among other things, organizations can position themselves to satisfy the DOJ's expectations without sacrificing any of the benefits that AI development and deployment offer. The time for companies to act is now — before misconduct occurs and prosecutors begin applying the ECCP framework to make investigative and enforcement decisions.

Stay tuned to Haynes Boone's News page for the latest updates on agency guidance and best practices concerning the use of AI and other emerging technologies. For further guidance, contact a member of Haynes Boone's White Collar and Investigations, Criminal Investigations and Defense, or AI and Deep Learning practice groups.

---

[1] The ECCP incorporates the comprehensive definition of AI from OMB Memorandum M-24-10 and clarifies that it encompasses machine learning, deep learning, reinforcement learning, transfer learning and generative AI. The DOJ also specifies that "no system should be considered too simple to qualify as a covered AI system due to a lack of technical complexity," meaning companies cannot escape scrutiny by characterizing their AI tools as unsophisticated.

[2] *See Louis v. SafeRent Solutions, LLC*, No. 1:22-cv-10800 (D. Mass.).

[3] *See United States v. RealPage Inc.*, No. 1:24-cv-00710 (M.D.N.C.); *Cornish-Adebiyi v. Caesars Entm't, Inc.*, No. 1:23-cv-02536 (D.N.J.); *In re RealPage, Inc., Rental Software Antitrust Litig. (No. II)*, No. 3:23-md-03071 (M.D. Tenn.); *Duffy v. Yardi Sys., Inc.*, No. 2:23-cv-01391 (W.D. Wash.).