Published on *The National Law Review* https://natlawreview.com

DOJ Makes Key Revisions to Corporate Compliance Program Guidance

Article By:

Anne Elkins Murray

Caitlin Sheard

Amy Bentsen (Boring)

Ashley Hoff

William W. Hameline

On September 23, 2024, the US Department of Justice (DOJ) updated its Evaluation of Corporate Compliance Programs guidance (ECCP). Changes to the ECCP build on themes that the DOJ has been emphasizing for some time, including risk assessment, compliance empowerment, effective reporting structures, and continuous improvement. The most recent updates encourage companies to:

- **Manage evolving risks associated with technology, including artificial intelligence (AI);**
- **Empower compliance with data and resources;**
- **Ensure the organization has a speak-up culture and whistleblower protections; and**
- **Learn from others, reevaluate risks, and make compliance enhancements.**

In Depth

WHAT'S NEW

Managing Evolving Risks Associated With Technology, Including AI

The DOJ has long expected companies to review and update their compliance programs to account for emerging risks. With this latest version of the ECCP, the department expands this concept to risks associated with the use of new and emerging technologies, including AI. The revised guidance instructs prosecutors to scrutinize how companies use AI, assess related risks, and take proactive measures to prevent AI-enabled criminal schemes.

What type of compliance risks might companies encounter when using AI and other emerging technologies? In recent remarks, Principal Deputy Assistant Attorney General Nicole M. Argentieri suggested that “false approvals and documentation generated by AI” could be used to facilitate criminal activity. Companies also risk relying on inaccurate data leveraged from untested or unreliable technologies. To protect against such risks, the DOJ expects companies to:

- Assess and mitigate risks associated with the use of new or emerging technologies, including AI;
- Develop and implement a governance strategy regarding the use of new technologies;
- Implement controls to monitor and ensure that AI and similar technologies are being used for their intended purpose in compliance with applicable laws and the company’s code of conduct, and to confirm the accuracy and reliability of the data leveraged from such technologies;
- Consider an appropriate baseline of human decision-making when using AI; and
- Train employees on the use of AI and other emerging technologies.

While the DOJ intensifies its focus on AI, companies should consider these updates to the ECCP when implementing any novel technology solution for business or compliance purposes. This is particularly important given that the DOJ has increasingly encouraged companies to leverage data and technology in their compliance programs, as discussed below.

Empowering Compliance With Data and Resources

The DOJ views data as a powerful tool to prevent and detect misconduct. Prior versions of the ECCP encouraged the use of data to monitor and test policies, controls, and transactions. The revised ECCP heightens this focus, asking:

- Whether compliance personnel have timely access to relevant data sources;
- Whether the company is leveraging data analytics to create efficiencies in compliance operations and measure compliance program effectiveness; and
- How the company is managing data quality and measuring the accuracy, precision, and recall of data analytics models.

Data is critical to facilitating testing of the compliance program, which is another focus area of the revised ECCP. For instance, the updated guidance suggests that companies should:

- Confirm that employees know how to access relevant policies (which may involve tracking policy access or testing knowledge through surveys or other means);
- Evaluate employees’ engagement with training content (which may involve collecting data on completion rates and comprehension);
- Leverage data to evaluate third-party risk during the relationship; and
- Take steps to measure the success and effectiveness of their compliance programs.

The revised ECCP also newly emphasizes “proportionate resource allocation,” which suggests that

companies should empower compliance and risk management functions with the same level of technology and resources available to commercial teams.

Protecting Whistleblowers and Promoting a Speak-Up Culture

Whistleblowers are having more than a moment. Companies have raced to amend policies and procedures as the patchwork of European whistleblower laws grows and evolves in the wake of the European Union Whistleblower Directive. On this side of the pond, US government agencies continue to have success with whistleblower programs. In 2023 alone, the Securities and Exchange Commission's whistleblower program generated more than 18,000 whistleblower tips and nearly $600 million in awards. It is, therefore, no surprise that the DOJ implemented its own Corporate Whistleblower Awards Pilot Program earlier this year to incentivize information sharing with the department. Despite being in place for less than a month, the program has already garnered tips from over 100 individuals.

Against this backdrop, the revised ECCP includes a new section titled "Commitment to Whistleblower Protection and Anti-Retaliation," which reinforces the need to invest in a speak-up culture. Receiving internal reports of potential misconduct enables companies to investigate and stop misconduct, consider disclosure, and make compliance program enhancements. To facilitate reports, companies must establish internal reporting channels and an anti-retaliation policy. Training on internal reporting options and requirements is paramount. The revised ECCP goes further, asking:

- Whether companies are training not just on internal reporting avenues but also on external whistleblower protection laws, whistleblower programs, and regulatory regimes;
- Whether companies' practices "tend to chill" reporting;
- Whether employees involved in misconduct are treated differently based on whether they internally reported misconduct;
- How companies "assess employees' willingness to report misconduct"; and
- Whether companies "incentivize reporting of potential misconduct."

Companies should think creatively about internal reporting. If you review any company's code of conduct, you will likely encounter a section requiring employees to report potential violations of the law, code, or policy. The DOJ's recent updates to the ECCP call for companies to go even further.

Taking a Broad View of Lessons Learned

Companies must learn from both their own issues and those of others. The DOJ's updates to the ECCP illustrate that companies cannot afford to have tunnel vision when determining their risk profile. Both internal and external circumstances should inform compliance programs. The revised ECCP emphasizes the importance of considering lessons learned by "other companies operating in the same industry and/or geographic region" when conducting risk assessments, designing and updating policies and procedures, and delivering tailored training.

Other Updates

- **Post-M&A integration**: Compliance and risk management personnel should be involved in post-transaction integration planning. The revised ECCP asks, "Does the company account for migrating or combining critical enterprise source planning systems as part of the integration process?"
- **Third-party management**: The revised ECCP instructs prosecutors to consider whether a

company's third-party management process allows for the review of vendors in a timely manner, emphasizing the need for efficiency in the process.
- **Training and communications**: Echoing existing guidance, the revised ECCP emphasizes that training and communications should be tailored to the particular needs, interests, and values of relevant employees.

LOOKING AHEAD

Now is the time to review your corporate compliance program. Consider whether your risk assessment methodology addresses the DOJ's focus areas. Assess whether there are opportunities to make enhancements to your corporate compliance program to navigate emerging technology, access to data, whistleblowers, and industry risks.

National Law Review, Volume XIV, Number 271

Source URL:https://natlawreview.com/article/doj-makes-key-revisions-corporate-compliance-program-guidance