KPMG

Regulatory Alert

Regulatory Insight Center

DOJ expands focus on effective compliance programs

Heightened attention to effective compliance programs.

Key points

- The Department of Justice Criminal Division released guidelines to evaluate the effectiveness of corporate compliance programs.
- Organizations should consider investments in the program, improvements to the program and internal controls systems to prevent or detect misconduct as well as to address/remediate identified misconduct, and testing to demonstrate the effectiveness of improvements.
- Ethics, conduct, and culture feature prominently throughout the guidelines, elevating the expectations for organizations to expand and integrate these areas.

The U.S. Department of Justice Criminal Division released new guidelines for evaluating the effectiveness of corporate compliance programs. The guidance covers topics the Criminal Division has found relevant in evaluating corporate compliance, and is organized around three overarching questions: 1) is the program well-designed?, 2) is the program effectively implemented?, and 3) does the program actually work? Attention is directed toward an organization's level of investment in its compliance program, improvements to prevent or detect future misconduct, and integration of a culture of ethics and compliance with day-to-day operations.

1. **Is the program well-designed?** Critical factors in evaluating a compliance program include whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees, is enforced by management, and is well-integrated into the company's operations and workforce. Topics that should be evaluated include:
   - **Risk assessment**. The risk assessment is considered the starting point of an evaluation. The compliance program should be designed to detect the types of misconduct most likely to occur in the organization's line of business and regulatory environment, including factors such as location of operations, industry sector, competitiveness of the market, potential clients and business partners, transactions with foreign governments/payments to foreign officials, use of third parties, gifts/travel/entertainment expenses, and charitable/political donations. Risk assessments should be used to tailor the compliance program, and the criteria periodically updated and continuously refined "in light of lessons learned."
   - **Policies and procedures**. Policies and procedures should aim to reduce risk identified through risk assessments and to give content and effect to ethical norms, including the organization's code of conduct, by incorporating the organization's culture of compliance into day-to-day operations. Policies and procedures should be communicated to all employees and relevant third parties, and any linguistic or other barriers to foreign employee access should be addressed.

- **Training and communications**. Organizations should ensure that policies and procedures are integrated through training for all directors, officers, relevant employees, and agents and partners (as appropriate). Organizations should also: be able to explain the rationale for how training is conveyed (such as in person or online delivery); incorporate lessons learned from prior compliance incidents; and measure the effectiveness of the training.
- **Confidential reporting and investigations**. The compliance program must include a mechanism for employees to anonymously or confidentially report allegations of misconduct. Complaint handling measures should create a workplace atmosphere without fear of retaliation and with protection for whistleblowers. Further, complaints should be routed to the proper personnel and investigations timely completed with appropriate follow up and discipline. Investigations should analyze misconduct for root causes (e.g., patterns of misconduct or other red flags of compliance weaknesses.)
- **Third-party management**. Compensation of third parties should be commensurate with the work being provided in that industry and geographic region; contracts must specifically describe the services being performed; and the third party must actually be performing the work. Organizations should engage in ongoing monitoring of the third-party relationships through updated due diligence, training, audits, and/or annual compliance certifications. Organizations should also consider tracking red flags identified through due diligence, requiring audit rights to be set out in the contract (and exercising those audit rights), and tracking rejected and terminated parties to ensure they do not re-enter the organization.
- **Mergers and acquisitions**. The compliance program should include comprehensive due diligence of acquisition targets. "The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization."

2. **Is the program effectively implemented?** The program must be more than a "paper program" and should be actively implemented, reviewed, and revised, as appropriate, with sufficient staff and clear management support. Factors to be considered include:
   - **Management commitment**. Management should create and foster a "culture of ethics and compliance with the law," demonstrate "conduct at the top" with rigorous adherence by example, and clearly convey, in unambiguous terms, the firm's ethical standards, including consequences for misconduct. Compliance should have access to the board of directors.
   - **Autonomy and resources**. The compliance function should have sufficient seniority within the organization, sufficient staffing resources and expertise, and autonomy from management, including direct access to the board of directors.
   - **Incentives and disciplinary measures**. The organization should convey that unethical conduct will not be tolerated and the program should have disciplinary procedures in place to address misconduct as well as failure to take steps to prevent or detect misconduct. Disciplinary measures should be enforced consistently across the organization and commensurate with the violations.

3. **Does the program actually work?** An assessment of whether a program is effective in the event of misconduct should consider whether and how the misconduct was detected, what resources were in place to investigate, and the nature and thoroughness of remedial efforts. The effectiveness of the program should be assessed over time, including whether the program is evolving to address existing and changing compliance risks. Factors to be considered include:
   - **Continuous improvement, periodic testing, and review**. The organization must engage in meaningful efforts to review the compliance program and ensure it is not stale, as well as to promote improvement and sustainability. Reviews should include gap analyses to determine if particular areas of risk are not sufficiently addressed in the policies, controls, or training.
   - **Investigation**. Investigations of any allegations or suspicions of misconduct by the organization, its employees, or agents should be conducted in a timely and thorough manner, with established procedures for documenting the organization's response, including disciplinary or remediation measures taken.

– **Analysis and remediation of underlying misconduct**. Organization should conduct a root cause analysis, including the extent and pervasiveness of misconduct, the seriousness, duration, and frequency of the misconduct, and remedial actions taken. Consideration should be given to: why the controls failed, vendor selection (if appropriate), prior indicators of control failures or allegations of misconduct, and management accountability.

KPMG perspectives

The DOJ guidance provides all federal prosecutors guidance to assess an organization's compliance program irrespective of industry, activities, or potential misconduct being investigated or remediated. The guidance fundamentally asks if the program is well designed, effectively implemented, and working in practice. Notably, the guidance directly links ethics with compliance, so that all companies should continue to strengthen corporate culture initiatives and controls. The guidance sets forth minimum expectations as a company looks to evaluate and enhance existing compliance programs and may also be utilized as a foundation in assessing third parties and during merger and acquisition and due diligence processes. It should be noted that much of the guidance is not "new" but rather a codification of prior expectations and a reiteration of the importance of ethics and compliance programs to help prevent and quickly detect potential misconduct. Effective ethics and compliance programs may help to determine the nature and severity of penalties.

The Department of the Treasury's Office of Foreign Assets Control (OFAC) separately released a framework for sanctions compliance that is applicable to U.S. organizations and foreign entities doing business in or with U.S. parties or goods. The OFAC guidance stresses many of the same points highlighted by DOJ with regard to evaluating compliance programs. KPMG's Regulatory Alert on the OFAC release can be accessed here.

KPMG's 2019 CCO Survey highlights the areas leading chief ethics and compliance officers say they plan to focus on and integrate in the next year. Click here to access the survey.

For additional information please contact our Regulatory and Compliance Transformation team leads:

— Dan Click (Consumer Markets/Industrial Manufacturing/Retail)
— Michael Lamberth (Insurance)
— Brent McDaniel (Energy)
— Anthony Monaco (Government)
— Jaime Pego (Healthcare & Life Sciences)
— Todd Semanco (Banking & Capital Markets)
— Jennifer Shimek (Healthcare & Life Sciences)
— Guido van Drunen (Technology, Media, and Telecommunications)

Amy Matsuo
Principal and National Lead
Regulatory Insights Lead
Regulatory and Compliance Transformation Lead
T: 919-664-7302
E: amatsuo@kpmg.com

Contributing authors:
Amy Matsuo, Principal and National Lead, Regulatory Insights

Karen Staines, Director, Financial Services Regulatory Insight Center

Nicole Stryker, Director, Operations and Compliance Risk

kpmg.com/socialmedia