COSMOS
Navigate the Compliance Universe

Compliance Today - September 2019
New Department of Justice guidance on evaluating corporate compliance programs

By Thomas E. Herrmann, JD

Thomas E. Herrmann (therrmann@strategicm.com) is a Managing Senior Consultant at Strategic Management Services LLC in Alexandria, VA.

In April 2019, the U.S. Department of Justice (DOJ) issued updated guidance for federal prosecutors on the process and considerations related to the Evaluation of Corporate Compliance Programs.[1] The new guidelines are intended to assist criminal prosecutors in assessing the effectiveness of a corporate compliance program when determining the appropriate enforcement and resolution of a criminal case. Valuable information is provided for compliance professionals as to what DOJ considers important in designing, developing, and implementing a corporate compliance program, and evaluating the effectiveness of an existing compliance program.

The new DOJ guidelines are the latest issuance of information relating to corporate compliance programs by the federal government since the Office of Inspector General (OIG) in the U.S. Department of Health and Human Services (DHHS) published its series of Compliance Program Guidances (CPG) for various sectors of the healthcare industry between 1997 and 2008.[2] The new guidelines do not introduce any dramatically new concepts related to corporate compliance programs, but they highlight the current DOJ view on considerations and priorities related to the evaluation of an organization's compliance program. Moreover, the guidelines are not limited to healthcare organizations, but are applicable to corporate compliance programs in all business sectors.

DOJ notes at the outset that it "does not use any rigid formula to assess the effectiveness of corporate compliance programs," and "recognize[s] that each company's risk profile and solutions to reduce its risks warrant particularized evaluation," with "an individualized determination" in each case. It goes on to make the point that "there are 'common questions' that need to be asked and answered in making the 'individualized determination' with respect to a corporation's compliance program effectiveness." DOJ explains that the new guidance is intended "to assist prosecutors in making informed decisions as to whether, and to what extent, [a] corporation's compliance program was effective at the time of [an] offense, and is effective at the time of a [DOJ] charging decision or resolution . . . ."[3]

DOJ focuses on three "fundamental questions" that need to be asked:

1. Is a corporation's compliance program well designed?
2. Is the compliance program being applied earnestly and in good faith?
3. Does a corporation's compliance program work in practice?[4]

To address these three lines of inquiry, the DOJ has identified key issues and compliance program elements that need to be assessed.

1. Is the corporation's compliance program well designed?

First and foremost, the DOJ advises that the structure and comprehensiveness of an organization's compliance program needs to be evaluated.

Risk assessment

A corporate compliance program's evaluation should begin with an assessment of the risk assessment process utilized by the organization. "The starting point for an . . . evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks."[5]

An organization's compliance program should be structured and implemented to focus on identified high-risk areas. DOJ recommends that consideration be given as to:

> Whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.[6]

The initial issue to be assessed is the organization's risk assessment process and subsequent steps to tailor its compliance program appropriately to address and mitigate risks. In addressing this key concern, the following questions should be asked:

- What methodology does a company use to identify, analyze, and address high-risk areas?
- Does the company devote resources and scrutiny to high-risk areas?
- Does the company's risk assessment undergo regular and periodic review and updating as necessary?

Policies and procedures

The DOJ goes on to note, "Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process."[7]

Therefore, the assessment of a corporation's compliance program needs to include a review of its code of conduct (Code), as well as a review of established policies and procedures that "incorporate the culture of compliance into its day-to-day operations."[8]

Questions to be addressed include:

- Does the Code set forth a company's commitment to compliance with applicable laws, regulations, and company standards/requirements?
- Is the Code accessible and applicable to all company stakeholders (e.g., board members, senior executives, employees, and contractors)?
- Are employees/contractors required to certify to receipt, review, and adherence to the Code?

- Is there an established and consistent process for the development and implementation of policies and procedures?
- Do policies and procedures address key risk areas and compliance principles?
- Are policies and procedures accessible to all employees and contractors?
- Are policies and procedures integrated into the organization's core operations?

Training and education

DOJ also advises that critical to an effective compliance program is appropriate training and education. A company needs to ensure that policies and procedures are integrated and operationalized through initial and periodic training of employees, contractors, and other stakeholders. Further, specialized risk-based training needs to be developed and provided for high-risk and control employees.

Among the questions to be considered are:

- Is training offered in a form and language appropriate to the audience?
- Is training provided online and/or in person?
- How is the effectiveness of training measured?
- Are employees/contractors required to certify to completion of training?
- How does the company address situations where an employee fails to either take training or pass a content-related quiz?
- Does training address key compliance principles and risk areas?
- Is specialized training provided to employees engaged in high-risk areas?
- Do managers and supervisors receive supplemental compliance training?

Communications

The DOJ guidance states that "another hallmark of a well-designed compliance program is appropriately tailored . . . communications."[9]

A company needs to ensure that information about its compliance program and employee/stakeholder obligations are properly communicated. In considering this issue, the following questions should be addressed:

- How does a company communicate to stakeholders about its compliance program and key risk areas?
- What resources are made available to stakeholders to give guidance regarding applicable policies and procedures, as well as key risk areas?
- How has the company communicated its standards regarding discipline/enforcement for misconduct and/or noncompliance?

Confidential reporting structure

A key compliance element identified by DOJ is the existence of a system enabling confidential reporting of compliance concerns or issues. "Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct.[10]

A company needs to ensure that it has a reliable and easy way for employees and others to communicate compliance concerns in an anonymous and/or confidential manner. In addressing this issue, the following questions should be answered:

- Has a company established a mechanism by which employees and others can anonymously or confidentially report suspected or actual misconduct/compliance issues?
- Has a company communicated its commitment to a workplace that does not tolerate retaliation or retribution for good faith reporting of compliance issues?
- Has a company established policies and procedures to protect "whistleblowers" from retaliation or retribution?
- Does a company follow up on its hotline/helpline communications in a comprehensive and timely manner, and track them from receipt to resolution?

Investigations

The DOJ guidance states that there also needs to be an assessment of a "company's processes for handling investigations . . . including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline."[11]

A company should ensure that it has a standard and reliable process for the receipt and comprehensive investigation of all credible complaints. In assessing this issue, the following questions should be addressed:

- Does a company have a process for evaluating complaints and determining which ones merit further investigation?
- Does a company have a system for tracking complaints from receipt through investigation to finding/resolution/remedial action?
- Does a company have a system for ensuring that investigations are appropriately handled and properly documented?
- Does a company have a process for self-reporting violations and following up/tracking corrective actions?

Third-party relationships

DOJ also opines that "a well-designed compliance program should apply risk-based due diligence to its third-party relationships."[12]

In addressing this principle, the following questions should be considered:

- Is there a process for applying risk-based due diligence to third-party relationships?
- Are there adequate controls to ensure that contract terms and relationships are appropriate?

- Does a company assess the qualifications and associations of third-party partners, contractors, agents, distributors, and consultants?
- Does a company undertake ongoing monitoring of third-party relationships through training, audits, and/or compliance certifications?
- Does a company take action where a third-party contractor or vendor is noncompliant?

Mergers and acquisitions

And finally, DOJ advises that "a well-designed compliance program should include comprehensive due diligence of any acquisition targets."[13]

In assessing this criterion, the following questions should be addressed:

- Is comprehensive due diligence conducted related to any potential acquisition or merger?
- How is compliance addressed during the acquisition, merger, and integration process?
- How does a company track and remediate misconduct or risks identified during the due diligence process?