U.S. Department of Justice
Criminal Division
Fraud Section

Evaluation of Corporate Compliance Programs

Introduction

The Principles of Federal Prosecution of Business Organizations in the United States Attorney's Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporate entity, determining whether to bring charges, and negotiating plea or other agreements. These factors, commonly known as the "Filip Factors," include "the existence and effectiveness of the corporation's pre-existing compliance program" and the corporation's remedial efforts "to implement an effective corporate compliance program or to improve an existing one."

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation that triggers the application of the Filip Factors, the Fraud Section does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case.

There are, however, common questions that we may ask in making an individualized determination. This document provides some important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program. The topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue.

Many of the topics below also appear in the United States Attorney's Manual ("USAM"), in the United States Sentencing Guidelines ("USSG"), in Fraud Section corporate resolution agreements, in *A Resource Guide to the U.S. Foreign Corrupt Practices Act* ("FCPA Guide") published in November 2012 by the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC), in the Good Practice Guidance on Internal Controls, Ethics, and Compliance adopted by the Organization for Economic Co-operation and Development ("OECD") Council on February 18, 2010, and in the Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook") published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank.

Sample Topics and Questions

1. Analysis and Remediation of Underlying Misconduct

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? What systemic issues were identified? Who in the company was involved in making the analysis?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations involving similar issues? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

2. Senior and Middle Management[1]

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged the type of misconduct in question? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How does the company monitor its senior leadership's behavior? How has senior leadership modelled proper behavior to subordinates?

- **Shared Commitment** – What specific actions have senior leaders and other stakeholders (*e.g.*, business and operational managers, Finance, Procurement, Legal, Human Resources) taken to demonstrate their commitment to compliance, including their remediation efforts? How is information shared among different components of the company?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

3. Autonomy and Resources[2]

- **Compliance Role** – Was compliance involved in training and decisions relevant to the misconduct? Did the compliance or relevant control functions (*e.g.*, Legal, Finance, or Audit) ever raise a concern in the area where the misconduct occurred?

- **Stature** – How has the compliance function compared with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions?

- **Experience and Qualifications** – Have the compliance and control personnel had the appropriate experience and qualifications for their roles and responsibilities?

- **Autonomy** – Have the compliance and relevant control functions had direct reporting lines to anyone on the board of directors? How often do they meet with the board of directors? Are members of the senior management present for these meetings? Who reviewed the performance of the compliance function and what was the review process? Who has determined compensation/bonuses/raises/hiring/termination of compliance officers? Do the compliance and relevant control personnel in the field have reporting lines to headquarters? If not, how has the company ensured their independence?

- **Empowerment** – Have there been specific instances where compliance raised concerns or objections in the area in which the wrongdoing occurred? How has the company responded to such compliance concerns? Have there been specific transactions or deals that were stopped, modified, or more closely examined as a result of compliance concerns?

- **Funding and Resources** – How have decisions been made about the allocation of personnel and resources for the compliance and relevant control functions in light of the company's risk profile? Have there been times when requests for resources by the compliance and relevant control functions have been denied? If so, how have those decisions been made?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? What has been the rationale for doing so? Who has been involved in the decision to outsource? How has that process been managed (including who oversaw and/or liaised with the external firm/consultant)? What access level does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

4. Policies and Procedures[3]

a. Design and Accessibility

- **Designing Compliance Policies and Procedures** – What has been the company's process for designing and implementing new policies and procedures? Who has been involved in the design of policies and procedures? Have business units/divisions been consulted prior to rolling them out?

- **Applicable Policies and Procedures** – Has the company had policies and procedures that prohibited the misconduct? How has the company assessed whether these policies and procedures have been effectively implemented? How have the functions that had ownership of these policies and procedures been held accountable for supervisory oversight?

- **Gatekeepers** – Has there been clear guidance and/or training for the key gatekeepers (*e.g.*, the persons who issue payments or review approvals) in the control processes relevant to the misconduct? What has been the process for them to raise concerns?

- **Accessibility** – How has the company communicated the policies and procedures relevant to the misconduct to relevant employees and third parties? How has the company evaluated the usefulness of these policies and procedures?

b. **Operational Integration**

- **Responsibility for Integration** – Who has been responsible for integrating policies and procedures? With whom have they consulted (*e.g.*, officers, business segments)? How have they been rolled out (*e.g.*, do compliance personnel assess whether employees understand the policies)?

- **Controls** – What controls failed or were absent that would have detected or prevented the misconduct? Are they there now?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Approval/Certification Process** – How have those with approval authority or certification responsibilities in the processes relevant to the misconduct known what to look for, and when and how to escalate concerns? What steps have been taken to remedy any failures identified in this process?

- **Vendor Management** – If vendors had been involved in the misconduct, what was the process for vendor selection and did the vendor in question go through that process? See further questions below under Item 10, "Third Party Management."

5. <u>Risk Assessment</u>[4]

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faced?

- **Information Gathering and Analysis** – What information or metrics has the company collected and used to help detect the type of misconduct in question? How has the information or metrics informed the company's compliance program?

- **Manifested Risks** – How has the company's risk assessment process accounted for manifested risks?

6. **Training and Communications**[5]

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees that addressed the risks in the area where the misconduct occurred? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the intended audience? How has the company measured the effectiveness of the training?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position on the misconduct that occurred? What communications have there been generally when an employee is terminated for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

7. **Confidential Reporting and Investigation**[6]

- **Effectiveness of the Reporting Mechanism** – How has the company collected, analyzed, and used information from its reporting mechanisms? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Has the company's investigation been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

8. Incentives and Disciplinary Measures[7]

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and when did they occur? Were managers held accountable for misconduct that occurred under their supervision? Did the company's response consider disciplinary actions for supervisors' failure in oversight? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the type(s) of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

- **Human Resources Process** – Who participated in making disciplinary decisions for the type of misconduct at issue?

- **Consistent Application** – Have the disciplinary actions and incentives been fairly and consistently applied across the organization?

- **Incentive System** – How has the company incentivized compliance and ethical behavior? How has the company considered the potential negative compliance implications of its incentives and rewards? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations?

9. Continuous Improvement, Periodic Testing and Review[8]

- **Internal Audit** – What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

10. Third Party Management [9]

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – What was the business rationale for the use of the third parties in question? What mechanisms have existed to ensure that the contract terms specifically described the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the third party's incentive model against compliance risks? How has the company monitored the third parties in question? How has the company trained the relationship managers about what the compliance risks are and how to manage them? How has the company incentivized compliance and ethical behavior by third parties?

- **Real Actions and Consequences** – Were red flags identified from the due diligence of the third parties involved in the misconduct and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues? How has the company monitored these actions (*e.g.*, ensuring that the vendor is not used again in case of termination)?

11. Mergers and Acquisitions (M&A) [10]

- **Due Diligence Process** – Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What has been the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures at new entities?

[1] USSG § 8B2.1(b)(3); FCPA Guide, p.57; USAM 9-28.800 Comment; OECD Handbook, C.1, p.16 *et seq*.

[2] USSG § 8B2.1(2)(B)-(C); FCPA Guide, p.58; USAM 9-28.800 Comment; OECD Handbook, C.3, p. 23 *et seq*.

[3] USSG § 8B2.1(b)(1); FCPA Guide, pp.57-58; OECD Handbook, C.4 and C.5, p.27 *et seq*.

[4] USSG § 8B2.1(b)(5)(7) and (c); USAM 9-28.800 Comment; OECD Handbook, B, p.10 *et seq*.

[5] USSG § 8B2.1(b)(4); FCPA Guide p. 59; USAM 9-28.800 Comment; OECD Handbook, C.8, p. 54 *et seq*.

[6] USSG § 8B2.1(b)(5)(C); FCPA Guide, p. 61; OECD Handbook, C.10, p.60 *et seq*.

[7] USSG § 8B2.1(b)(6); FCPA Guide, pp.59-60; USAM 9-28.800 Comment; OECD Handbook, C.11, p. 68 *et seq*.

[8] USSG § 8B2.1(b)(5)(A)(B); FCPA Guide, pp.61-62; USAM 9-28.800 Comment; OECD Handbook, C.12, pp.72 *et seq*.

[9] FCPA Guide, p.60-66; OECD Handbook, C.6, pp.38 *et seq*.

[10] FCPA Guide, p.62.