Criminal Division's Evaluation of Corporate Compliance Programs

September 2024 Updates Review

In September 2024, the Criminal Division of the U.S. Department of Justice (DOJ) published the latest revisions to the "Evaluation of Corporate Compliance Programs (ECCP)."

Although intended to direct prosecutors in evaluating corporate compliance programs to reach an appropriate resolution following a criminal investigation, the ECCP also often serves as a helpful resource for legal and compliance teams to evaluate the adequacy and effectiveness of their own corporate compliance programs.

As with previous versions, the ECCP builds upon three "fundamental questions:"

1. Is the corporate compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?
3. Does the corporate compliance program work in practice?

The latest revisions to the ECCP direct prosecutors to consider several new questions in evaluating corporate compliance programs, including in the following newly added areas: disruptive technology risks, such as artificial intelligence (AI); whistleblower protections; data resources and access; and a company's ability to learn from past mistakes.

Disruptive technology risks

The most comprehensive updates to the latest revisions of the ECCP highlight the DOJ's enhanced focus on mitigating risks associated with disruptive technologies, including AI. In March 2023, Deputy Attorney General Lisa Monaco directed the Criminal Division to "incorporate assessment of disruptive technology risks, including risks associated with AI," in the ECCP.

As with any corporate criminal resolution, prosecutors always assess how the compliance program mitigates significant risks. "For a growing number of businesses, that now includes the risk of misusing AI," Monaco noted.

Additionally, Monaco forewarned that prosecutors will seek stiffer sentences for offenses "made significantly more dangerous by the misuse of AI." Specific examples of AI misuse could include false approvals or AI-generated documentation.

Compliance officers and compliance programs play an important role in mitigating risks due to the company's and employees' use of disruptive technologies. Prosecutors will consider, for example, whether compliance controls and tools are in place that can "confirm the accuracy or reliability of data used by the business," remarked Principal Deputy Assistant Attorney General Nicole Argentieri.

They also will examine "whether the company is monitoring and testing its technology to evaluate if it is functioning as intended and consistent with the company's code of conduct," Argentieri said.

The revised ECCP has a new section directing prosecutors to assess how the company and the compliance program manage emerging risks. New questions compliance officers should consider include:

- Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management (ERM) strategies?
- What is the company's approach to governance regarding the use of new technologies, such as 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 technologies, 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?

Prosecutors also will assess whether monitoring controls are in place to ensure the trustworthy use of AI, that it complies with applicable law and the company's values, and that it's being used for its intended purposes. Additionally, prosecutors will assess human decision-making processes; how accountability for AI use is monitored and enforced; and how employees are trained to responsibly use AI.

Whistleblower protections

In addition to AI, the DOJ is increasingly paying closer attention to how compliance programs foster a speak-up culture. In August 2024, the Criminal Division launched its Corporate Whistleblower Awards Pilot Program. Under the pilot program, individuals who provide the DOJ with "original information in writing" regarding corporate misconduct that leads to criminal or civil forfeiture exceeding $1 million in net proceeds may be eligible for an award.

> *"Our prosecutors will closely consider the company's commitment to whistleblower protection and anti-retaliation by assessing policies and training, as well as treatment of employees who report misconduct," Argentieri said.*

As described in the program guidance, the information must pertain to one of the following subject-matter areas: (1) certain fraudulent schemes or money-laundering schemes committed by financial institutions, their insiders, or agents; (2) foreign corruption and bribery involving misconduct "by, through, or related to companies," including violations of the Foreign Extortion Prevention Act; or (3) violations committed by or through companies for bribes or kickbacks to domestic public officials.

Additionally, individuals may be eligible for a whistleblower award for reporting violations related to (a) "federal health care offenses and related crimes involving private or other non-public health care benefit programs, where the overwhelming majority of claims are submitted to private or other non-public health care benefit programs; (b) fraud against patients, investors, and other non-governmental entities in the health care industry, where the overwhelming majority of the actual or intended loss was to patients, investors, and other non-governmental entities; and (c) any other federal violations involving conduct related to health care not covered by the federal False Claims Act.

There are incentives for companies as well. Companies that voluntarily self-report within 120 days of receiving an internal whistleblower report may be eligible for a presumption of a declination under the Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy if the company reports to the DOJ first.

To revised ECCP complements the pilot program by incorporating new questions for prosecutors to evaluate regarding whistleblower protections. "Our prosecutors will closely consider the company's commitment to whistleblower protection and anti-retaliation by assessing policies and training, as well as treatment of employees who report misconduct," Argentieri said. "We will evaluate whether companies ensure that individuals who suspect misconduct know how to report it and feel comfortable doing so, including by showing that there is no tolerance for retaliation."

> *"We will evaluate whether companies ensure that individuals who suspect misconduct know how to report it and feel comfortable doing so, including by showing that there is no tolerance for retaliation."*

Championing for whistleblower and anti-retaliation protections is another area where compliance departments play an important role. It's also an area prosecutors will pay close attention to, in addition to "whether a company has fostered a speak-up culture," Argentieri stressed.

Conversely, where a whistleblower faces retaliation, the DOJ "will take all appropriate steps: The company will lose credit for cooperation and remediation and could face sentencing enhancements — and even prosecution — for obstruction of justice," she warned.

Data resources and access

Other significant revisions to the ECCP concern data resources and access. Under the revised ECCP, prosecutors will now assess whether compliance programs have "sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions."

Examples of questions they will now consider include:

- Do any impediments exist that limit or delay access to relevant sources of data? And, if so, what is the company doing to address the impediments?
- Do compliance personnel have knowledge of, and means to access, all relevant data sources in a reasonably timely manner?
- Is the company appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs?
- How is the company managing the quality of its data sources?
- How is the company measuring the accuracy, precision, or recall of any data analytics models it is using?

As part of this assessment, prosecutors also will consider "whether companies are putting the same resources and technology into gathering and leveraging data for compliance purposes that they are using in their business," Argentieri said.

Additionally, prosecutors will examine data access relative to third-party management. Specifically, the revised ECCP directs prosecutors to ask, "Does the third-party management process function allow for the review of vendors in a timely manner? How is the company leveraging available data to evaluate vendor risk during the course of the relationship with the vendor?"

> *...prosecutors also will consider "whether companies are putting the same resources and technology into gathering and leveraging data for compliance purposes that they are using in their business," Argentieri said.*

Compliance lessons learned

The updated ECCP further expands upon whether companies have learned from past mistakes, either their own or those of other companies operating in the same industry and/or geographical region. Prosecutors will be looking to see whether lessons learned have been reflected through remediation measures and updated policies and procedures.

Questions compliance officers and compliance programs should consider include, for example:

- Has the training addressed lessons learned from compliance issues faced by other companies operating in the same industry and/or geographical region?
- Has the company evaluated the employees' engagement with the training session and whether they have learned the covered subject matter?
- How and how often does the company measure the success of its compliance program?

The remainder of this document highlights the key revisions that have been incorporated into the September 2024 version of the ECCP, comparing it to its last iteration in March of 2023. Compliance officers are encouraged to review what new areas and key questions prosecutors will consider in evaluating the compliance program going forward. All companies are encouraged to use the ECCP as a framework against which to structure a robust corporate compliance program.

To download a copy of the latest version of the Evaluation of Corporate Compliance Programs, click here.

The following document was published and is managed by the U.S. Department of Justice's Criminal Division.
(Highlighted sections indicate changes from the previous version of the DOJ Guidance)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9- 28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. See U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future" to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division 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 a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?
3. Does the corporation's compliance program work in practice? See JM 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.1 The sample 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 and the circumstances of the company.2 Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

I. Is the Corporation's Compliance Program Well Designed?

The "critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct." JM 9-28.800.

Accordingly, prosecutors should examine the comprehensiveness of the compliance program, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to lines of reporting and communication, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

A. Risk Assessment

The starting point for a prosecutor's 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, including specific factors that mitigate the company's risk, and the degree to which the program devotes appropriate scrutiny and resources to the remaining spectrum of risks. This evaluation should account for emerging risks as internal and external circumstances impacting the company's risk profile evolve. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

Prosecutors should consider whether the program is appropriately "designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[ ]." JM 9-28.8003 For example, prosecutors should consider 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. Where relevant, prosecutors should consider the technology – especially new and emerging technology – that the company and its employees are using to conduct company business, whether the company has conducted a risk assessment regarding the use of that technology, and whether the company has taken appropriate steps to mitigate any risk associated with the use of that technology.

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." See, e.g., JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c)("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What features of the company reduce its exposure to such risks? Is the company's approach to risk management proactive or reactive? What information has the company identified and collected to help detect the type of misconduct in question? How has that information informed the company's compliance program?
- **Risk-Tailored Resource Allocation** – Does the company deploy its compliance resources in a risk-based manner, with greater scrutiny, applied to greater areas of risk?
- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?
- **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?
- **Management of Emerging Risks to Ensure Compliance with Applicable Law** – Does the company have a process for identifying and managing emerging internal and external risks that could potentially impact the company's ability to comply with the law, including risks related to the use of new technologies? How does the company assess the potential impact of new technologies, such as artificial intelligence (AI),4 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 (ERM) strategies? What is the company's approach to governance regarding the use of new technologies such as 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 technologies, 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? To the extent that the company uses AI and similar technologies in its business or as part of its compliance program, are controls in place to monitor and ensure its trustworthiness, reliability, and use in compliance with applicable law and the company's code of conduct? Do controls exist to

ensure that the technology 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?

B. Policies and Procedures

Any well-designed compliance program utilizes policies and procedures to give both content and effect to ethical norms and to mitigate risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Is there a process for updating policies and procedures to reflect lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region? Is there a process for updating policies and procedures to address emerging risks, including those associated with the use of new technologies? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape and the use of new technologies?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? Have the policies and procedures been published in a searchable format for easy reference? How does the company confirm that employees know how to access relevant policies? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise.

Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area(s) where misconduct

occurred? Have supervisory employees received different or supplementary training? 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 audience? Are the company's training and communications tailored to the particular needs, interests, and values of relevant employees? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Has the training addressed lessons learned from compliance issues faced by other companies operating in the same industry and/or geographical region? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Has the company evaluated the employees' engagement with the training session and whether they have learned the covered subject matter? How has the company addressed employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined 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?

D. Confidential Reporting Structure and Investigation Process

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. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has "established corporate governance mechanisms that can effectively detect and prevent misconduct." JM 9-28.800; see also U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company test whether employees are aware of the hotline and feel comfortable using it? Does the company encourage and incentivize reporting of potential misconduct or violation of company policy? Conversely, does the company use practices that tend to chill such reporting? How does the company assess employees' willingness to report misconduct? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Commitment to Whistleblower Protection and Anti-Retaliation** – Does the company have an anti-retaliation policy? Does the company train employees on both internal anti-retaliation policies and external anti-retaliation and whistleblower protection laws? To the extent that the company disciplines employees involved in misconduct, are employees who reported internally treated differently than others involved in misconduct who did not? Does the company train employees on internal reporting systems as well as external whistleblower programs and regulatory regimes?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party. In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9- 28.800.

- **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? Does the third-party management process function allow for the review of vendors in a timely manner? How is the company leveraging available data to evaluate vendor risk during the course of the relationship with the vendor?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe 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 compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third-party relationship managers about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

- **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

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

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? 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 is 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? Does the company account for migrating or combining critical enterprise resource planning systems as part of the integration process? To what extent did compliance and risk management functions play a role in designing and executing the integration strategy?
- **Post-Transaction Compliance Program** – What is the company's process for implementing and/or integrating a compliance program post-transaction? Does the company have a process in place to ensure appropriate compliance oversight of the new business? How is the new business incorporated into the company's risk assessment activities? How are compliance policies and procedures organized? Are post-acquisition audits conducted at newly acquired entities?

II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one "implemented, reviewed, and revised, as appropriate, in an effective manner." JM 9-28.800. In addition, prosecutors should determine "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts." JM 9- 28.800. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it." JM 9-28.800; see also JM 9-47.120(2)(c)(criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. See U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; *"[h]igh-level personnel* ... shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled ethical behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?
- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (e.g., business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?
- **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?

B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient qualifications, seniority, and stature (both actual and perceived) within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." Id. Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether "internal audit functions are conducted at a level sufficient to ensure their independence and accuracy," as an indicator of whether compliance personnel are in fact empowered and positioned to "effectively detect and prevent misconduct." JM 9-28.800. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); see also JM 9-28.800 (instructing prosecutors to evaluate whether "the directors established an information and reporting system in the organization reasonably designed to provide management and directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law"); U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- **Seniority and Stature** – How does the compliance function compare 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? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds? Does the company have a mechanism to measure the commercial value of investments in compliance and risk management?

- **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit or delay access to relevant sources of data and, if so, what is the company doing to address the impediments? Do compliance personnel have knowledge of and means to access all relevant data sources in a reasonably timely manner? Is the company appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs? How is the company managing the quality of its data sources? How is the company measuring the accuracy, precision, or recall of any data analytics models it is using?

- **Proportionate Resource Allocation** – How do the assets, resources, and technology available to compliance and risk management compare to those available elsewhere in the company? Is there an imbalance between the technology and resources used by the company to identify and capture market opportunities and the technology and resources used to detect and mitigate risks?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

C. Compensation Structures and Consequences for Management

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear consequence management procedures (procedures to identify, investigate, discipline and remediate violations of law, regulation, or policy) in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. See U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, prosecutors may consider whether a company has publicized disciplinary actions internally, where appropriate and possible, which can have valuable deterrent effects. Prosecutors may also consider whether a company is tracking data relating to disciplinary actions to measure effectiveness of the investigation and consequence management functions. This can include monitoring the number of compliance-related allegations that are substantiated, the average (and outlier) times to complete a compliance investigation, and the effectiveness and consistency of disciplinary measures across the levels, geographies, units or departments of an organization.

The design and implementation of compensation schemes play an important role in fostering a compliance culture. Prosecutors may consider whether a company has incentivized compliance by designing compensation systems that defer or escrow certain compensation tied to conduct consistent with company values and policies. Some companies have also enforced contract provisions that permit the company to recoup previously awarded compensation if the recipient of such compensation is found to have engaged in or to be otherwise responsible for corporate wrongdoing. Finally, prosecutors may consider whether provisions for recoupment or reduction of compensation due to compliance violations or misconduct are maintained and enforced in accordance with company policy and applicable laws.

Compensation structures that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance. At the same time, providing positive incentives, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership, can drive compliance. Prosecutors should examine whether a company has made working on compliance a means of career advancement, offered opportunities for managers and employees to serve as a compliance "champion", or made compliance a significant metric for management bonuses. In evaluating whether the compensation and consequence management schemes are indicative of a positive compliance culture, prosecutors should consider the following factors:

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? How transparent has the company been with the design and implementation of its disciplinary process? In circumstances where an executive has been exited from the company on account of a compliance violation, how transparent has the company been with employees about the terms of the separation? Are the actual reasons for the discipline communicated to employees in all cases? If not, why not? Is the same process followed for each instance of misconduct, and if not, why? Has the company taken steps to restrict disclosure or access to information about the disciplinary process? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Disciplinary Measures** – What types of disciplinary actions are available to management when it seeks to enforce compliance policies? Does the company have policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee? What policies and practices does the company have in place to put employees on notice that they will not benefit from any potential fruits of misconduct? With respect to the particular misconduct at issue, has the company made good faith efforts to follow its policies and practices in this respect?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why? What metrics does the company apply to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the organization?

- **Financial Incentive System** – Has the company considered the impact of its financial rewards and other incentives on compliance? Has the company evaluated whether commercial targets are achievable if the business operates within a compliant and ethical manner? What role does the compliance function have in designing and awarding financial incentives at senior levels of the organizations? How does the company incentivize compliance and ethical behavior? What percentage of executive compensation is structured to encourage enduring ethical business objectives? Are the terms of the bonus and deferred compensation subject to cancellation or recoupment, to the extent available under applicable law, in the event that non-compliant or unethical behavior is exposed before or after the award was issued? Does the company have a policy for recouping compensation that has been paid, where there was been misconduct? Have there been specific examples of actions taken (e.g., promotions or awards denied, compensation recouped, or deferred compensation cancelled) as a result of compliance and ethics considerations?

- **Effectiveness** – How has the company ensured effective consequence management of compliance violations in practice? What insights can be taken from the management of a company's hotline that provides indicia of its compliance culture or its management of hotline reports? How do the substantiation rates compare for similar types of reported wrongdoing across the company (i.e., between two or more different states, countries, or departments) or compared to similarly situated companies, if known? Has the company undertaken a root cause analysis into areas where certain conduct is comparatively over or under reported? What is the average time for completion of investigations into hotline reports and how are investigations that are addressed inconsistently managed by the responsible department? What percentage of the compensation awarded to executives who have been found to have engaged in wrongdoing has been subject to cancellation or recoupment for ethical violations? Taking into account the relevant laws and local circumstances governing the relevant parts of a compensation scheme, how has the organization sought to enforce breaches of compliance or penalize ethical lapses? How much compensation has in fact been impacted (either positively or negatively) on account of compliance-related activities?

III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. See U.S.S.G. § 8B2.1(a)("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts. Prosecutors should also consider whether the company's compliance program had a track record of preventing or detecting other instances of misconduct, and whether the company exercised due diligence to prevent and detect criminal conduct. See U.S.S.G. § 8B2.1(a)(1).

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the underlying misconduct and the degree of remediation needed to prevent similar events in the future. Prosecutors should also assess how the company has leveraged its data to gain insights into the effectiveness of its compliance program and otherwise sought to promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law. See U.S.S.G. § 8B2.1(a)(2).

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; see also JM 9-47-120(2)(c)(looking to "[t]he auditing of the compliance program to assure its effectiveness"). This can include analysis of how the company responded to other instances of misconduct in addition to how the company addressed reports of potential misconduct and risks over time. Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? 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 does internal audit conduct assessments in high-risk areas?
- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?
- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks? If the company is using new technologies such as AI in its commercial operations or compliance program, is the company monitoring and testing the technologies so that it can evaluate whether they are 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?
- **Measurement** – How and how often does the company measure the success and effectiveness of its compliance program?
- **Culture of Compliance** – How and how often does the company measure its culture of compliance? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?
- **Data and Transparency** – To what extent does the company have access to data and information to identify potential misconduct or deficiencies in its compliance program? Can the company demonstrate that it is proactively identifying either misconduct or issues with its compliance program at the earliest stage possible?

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **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** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?
- **Independence and Empowerment** – Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the company? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?

Messaging applications have become ubiquitous in many markets and offer important platforms for companies to achieve growth and facilitate communication. In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications. Policies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company. Prosecutors should consider how the policies and procedures have been communicated to employees, and whether the corporation has enforced the policies and procedures on a regular and consistent basis in practice. In conducting this evaluation, prosecutors should consider the following factors:

- **Communication Channels** – What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does that practice vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each? What is the rationale for the company's approach to determining which communication channels and settings are permitted?
- **Policy Environment** – What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced? What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the organization's ability to ensure security or monitor/access business-related communications? If the company has a "bring your own device" (BYOD) program, what are its policies governing preservation of and access to corporate data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies? How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications? Do the organization's policies permit the company to review business communications on BYOD and/or messaging applications? What exceptions or limitations to these policies have been permitted by the organization? If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?
- **Risk Management** – What are the consequences for employees who refuse the company access to company communications? Has the company ever exercised these rights? Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and exercise control over the communication channels used to conduct the organization's affairs? Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company's business needs and risk profile?

C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; see also JM 9-47.120(3)(c)("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; see also JM 9-47-120(2)(c)(looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

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

Prior Weaknesses – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

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?

Vendor Management – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

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? 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?

Accountability – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (e.g., number and types of disciplinary actions) on employee discipline relating to the types 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? Did the company take any actions to recoup or reduce compensation for responsible employees to the extent practicable and available under applicable law?