HCCA Compliance Essentials Workshop

Additional Resources

Resource 1

Acronyms

ABC's of Acronyms

AAMC – American Association of Medical Colleges
AAPCC – Adjusted Average per Capita Cost
ABN – Advance Beneficiary Notice
ACA – Affordable Care Act
ACC – Ambulatory Care Center
ACER – Annual Contractor Evaluation Report
ACR – Adjusted Community Rate
ADPL – Average Daily Patient Load
AG – Attorney General
AHIMA- American Health Information Management Association
APGs – Ambulatory Patient Groups
ASC - Ambulatory Surgery Center
BA – Business Associate
BAA - Business Associate Agreement
CAH – Critical Access Hospital
CAHPS – Consumer Assessment of Health Plan Survey
CCO – Chief Compliance Officer
CDC – Center for Disease Control and Prevention
CHC – Certified in Healthcare Compliance
CHPC – Certified in Privacy Compliance
CHRC – Certified in Healthcare Research Compliance
CIA – Corporate Integrity Agreement
CLIA – Clinical Laboratory Improvement Act
CMP – Competitive Medical Plan
CMS – Centers for Medicare & Medicaid Services
COP - Conditions of Participation
CPR – Customary, Prevailing and Reasonable
CPT – Current Procedure Terminology
CRO – Chief Risk Officer
CWW – Clinic without Walls
DA – District Attorney
DEA – Drug Enforcement Agency
DME – Durable Medical Equipment
DOJ – Department of Justice
DRG - Diagnosis Related Group
DSH – Disproportionate Share Adjustment
EMR/EHR – Electronic Medical Record/Electronic Health Record
EPO - Exclusive Provider Organization
ERIS – Employee Retirement Income Security Act
FBI – Federal Bureau of Investigation
FDA – The Food and Drug Administration is responsible for protecting the public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices; and by ensuring the safety of our nation's food supply, cosmetics, and products that emit radiation.
FERPA – Family Education Privacy Rights Act
FQHC – Federally Qualified Health Clinic
GAO – Government Accountability Offices

HCC – Hierarchal Condition Category (Medicare Advantage)
HCCA – Health Care Compliance Association
HCPCS - Health Care Common Procedure Coding System
HHRG – Home Health Resource Group (HHA)
HIM – Health Information Management
HIMS – Health Information Management Services
HIPAA – Health Insurance Portability and Accountability Act
HITECH – High Tech Rule under the HIPAA Privacy and Security Regulations
IDTF – Independent Diagnostic Testing Facility
IOM – Institute of Medicine: A nonprofit organization established in 1970 as a component of the US National Academy of Sciences that works outside the framework of government to provide evidence-based research and recommendations for public health and science policy.
IRF – Inpatient Rehabilitation Facility
LCD – Local Coverage Determination
LEIE - OIG's List of Eligible and Ineligible entities
LDS – Limited Data Set
MAC – Medicare Administrative Contractor (CMS)
MDS - Minimum Data Set (SNF)
MLR – Medical Loss Ratio
MSP – Medicare Secondary Payer
NPI – National Provider Identifier
NSF – National Science Foundation (NSF) is a United States government agency that supports fundamental research and education in all the non-medical fields of science and engineering. Its medical counterpart is the National Institutes of Health.
NUBC – National Uniform Billing Committee
OASIS - Outcomes and Assessment Information Set (HHA)
OCR – Office for Civil Rights
OHRP – The Office for Human Research Protections is a small office within the United States Department of Health and Human Services (DHHS), specifically the Office of the Assistant Secretary for Health in the Office of the Secretary of DHHS that deals with ethical oversights in clinical research.
OIG – Office Inspector General
PHARMA – pharmaceutical companies collectively as a sector of industry.
PHI – Protected Health Information
PHR – Personal Health Record
PI – Performance Improvement
PPACA – Patient Protection and Affordable Care Act
PRRB – Provider Reimbursement Review Board
PTO - Payment, Treatment, and Health Care Operations - An exception under the HIPAA Privacy Regulations that permits uses and disclosures of PHI
QMS – Quality Management System
RUG – Resource Utilization Groups (SNF)
SAM - System for Award Management
SCCE- Society of Corporate Compliance & Ethics
SDN – Specially Designated Nationals and Blocked Persons List
SDP – Self Disclosure Protocol
SCHIP - State Children’s Health Insurance Program
SCOTUS – Supreme Court of the United States
SFR – Significant Financial Risk

SNF – Skilled Nursing Facility
SUBC – State Uniform Billing Committee
TPO - Treatment, Payment and Health Care Operations - An exception under the HIPAA Privacy Regulations that permits uses and disclosures of PHI
TRICARE - Veteran's Federal Health Insurance
UCR – Usual, Customary and Reasonable
VBP – Valued Based Purchasing
WHO – World Health Organization

Resource 2

DOJ Compliance Guidance

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated September 2024)

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 permitting 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 [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment []." JM 9-28.800.[3] 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. *See* 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 [and prevent] 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?

- **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?

- **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, resourced, reviewed, and revised, as appropriate, in an effective manner. JM 9-28.800. In this regard, prosecutors should evaluate a corporation's method for assessing and addressing applicable risks and designing appropriate controls to manage these risks. 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. 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").

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated September 2024)

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. 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* 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 Consequence 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 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 organization? 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 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 has 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 provide 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 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? How does the company's hiring and incentive structure reinforce its commitment to ethical culture? 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 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?

---

[1] Many of the topics also appear in the following resources:

- Justice Manual ("JM")
    - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
    - JM 9-47.120 and the Criminal Division Corporate Enforcement Policy, *available at* https://www.justice.gov/criminal-fraud/file/1562831/download.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8#NaN.Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download; updated Memorandum entitled "Selection of Monitors in Criminal Division Matters,"

issued by Assistant Attorney General Kenneth A. Polite, Jr., on March 2, 2023, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.

- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (the Department of Justice's ("DOJ") Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).

- A Resource Guide to the U.S. Foreign Corrupt Practices Act ("FCPA Guide"), published in November 2012 by the DOJ and the Securities and Exchange Commission ("SEC"), *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

- 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, *available at* https://www.oecd.org/daf/anti-bribery/44884389.pdf.

- 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, *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.

- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ's Antitrust Division, *available at* https://www.justice.gov/atr/page/file/1182001/download.

- A Framework for OFAC Compliance Commitments, published in May 2019 by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), *available at* https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.

- AI Risk Management Framework, released on January 26, 2023, by the National Institute of Standards and Technology ("NIST"), *available at* https://www.nist.gov/itl/ai-risk-management-framework.

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

---

[3] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations, require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars. Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).

[4] The term "artificial intelligence" has the meaning set forth in the OMB Memo M-24-10 at pages 26-27, *available at* https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf, and includes the following:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

Additionally, the following technical context should guide the interpretation of the definition:

1. This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including, but not limited to, deep learning as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.
2. This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.

3. For this definition, no system should be considered too simple to qualify as a covered AI system due to a lack of technical complexity (*e.g.*, the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes).

This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

Resource 3

Federal Sentencing Guidelines

CHAPTER EIGHT - SENTENCING OF ORGANIZATIONS

Introductory Commentary

The guidelines and policy statements in this chapter apply when the convicted defendant is an organization. Organizations can act only through agents and, under federal criminal law, generally are vicariously liable for offenses committed by their agents. At the same time, individual agents are responsible for their own criminal conduct. Federal prosecutions of organizations therefore frequently involve individual and organizational co-defendants. Convicted individual agents of organizations are sentenced in accordance with the guidelines and policy statements in the preceding chapters. This chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.

This chapter reflects the following general principles:

First, the court must, whenever practicable, order the organization to remedy any harm caused by the offense. The resources expended to remedy the harm should not be viewed as punishment, but rather as a means of making victims whole for the harm caused.

Second, if the organization operated primarily for a criminal purpose or primarily by criminal means, the fine should be set sufficiently high to divest the organization of all its assets.

Third, the fine range for any other organization should be based on the seriousness of the offense and the culpability of the organization. The seriousness of the offense generally will be reflected by the greatest of the pecuniary gain, the pecuniary loss, or the amount in a guideline offense level fine table. Culpability generally will be determined by six factors that the sentencing court must consider. The four factors that increase the ultimate punishment of an organization are: (i) the involvement in or tolerance of criminal activity; (ii) the prior history of the organization; (iii) the violation of an order; and (iv) the obstruction of justice. The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility.

Fourth, probation is an appropriate sentence for an organizational defendant when needed to ensure that another sanction will be fully implemented, or to ensure that steps will be taken within the organization to reduce the likelihood of future criminal conduct.

These guidelines offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program. The prevention and detection of criminal conduct, as facilitated by an effective compliance and ethics program, will assist an organization in encouraging ethical conduct and in complying fully with all applicable laws.

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422). Amended effective November 1, 2004 (see Appendix C, amendment 673).

PART A - GENERAL APPLICATION PRINCIPLES

§8A1.1. Applicability of Chapter Eight

This chapter applies to the sentencing of all organizations for felony and Class A misdemeanor offenses.

Commentary

Application Notes:

1. *"Organization" means "a person other than an individual." 18 U.S.C. § 18. The term includes corporations, partnerships, associations, joint-stock companies, unions, trusts, pension funds, unincorporated organizations, governments and political subdivisions thereof, and non-profit organizations.*

2. *The fine guidelines in §§8C2.2 through 8C2.9 apply only to specified types of offenses. The other provisions of this chapter apply to the sentencing of all organizations for all felony and Class A misdemeanor offenses. For example, the restitution and probation provisions in Parts B and D of this chapter apply to the sentencing of an organization, even if the fine guidelines in §§8C2.2 through 8C2.9 do not apply.*

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422).

§8A1.2. Application Instructions - Organizations

(a) Determine from Part B, Subpart 1 (Remedying Harm from Criminal Conduct) the sentencing requirements and options relating to restitution, remedial orders, community service, and notice to victims.

(b) Determine from Part C (Fines) the sentencing requirements and options relating to fines:

(1) If the organization operated primarily for a criminal purpose or primarily by criminal means, apply §8C1.1 (Determining the Fine - Criminal Purpose Organizations).

(2) Otherwise, apply §8C2.1 (Applicability of Fine Guidelines) to identify the counts for which the provisions of §§8C2.2 through 8C2.9 apply. For such counts:

(A) Refer to §8C2.2 (Preliminary Determination of Inability to Pay Fine) to determine whether an abbreviated determination of the guideline fine range may be warranted.

(B) Apply §8C2.3 (Offense Level) to determine the offense level from Chapter Two (Offense Conduct) and Chapter Three, Part D (Multiple Counts).

(C) Apply §8C2.4 (Base Fine) to determine the base fine.

(D) Apply §8C2.5 (Culpability Score) to determine the culpability score. To determine whether the organization had an effective compliance and ethics program for purposes of §8C2.5(f), apply §8B2.1 (Effective Compliance and Ethics Program).

(E) Apply §8C2.6 (Minimum and Maximum Multipliers) to determine the minimum and maximum multipliers corresponding to the culpability score.

(F) Apply §8C2.7 (Guideline Fine Range - Organizations) to determine the minimum and maximum of the guideline fine range.

(G) Refer to §8C2.8 (Determining the Fine Within the Range) to determine the amount of the fine within the applicable guideline range.

(H) Apply §8C2.9 (Disgorgement) to determine whether an increase to the fine is required.

For any count or counts not covered under §8C2.1 (Applicability of Fine Guidelines), apply §8C2.10 (Determining the Fine for Other Counts).

(3) Apply the provisions relating to the implementation of the sentence of a fine in Part C, Subpart 3 (Implementing the Sentence of a Fine).

(4) For grounds for departure from the applicable guideline fine range, refer to Part C, Subpart 4 (Departures from the Guideline Fine Range).

(c) Determine from Part D (Organizational Probation) the sentencing requirements and options relating to probation.

(d) Determine from Part E (Special Assessments, Forfeitures, and Costs) the sentencing requirements relating to special assessments, forfeitures, and costs.

Commentary

Application Notes:

1. *Determinations under this chapter are to be based upon the facts and information specified in the applicable guideline. Determinations that reference other chapters are to be made under the standards applicable to determinations under those chapters.*

2. The definitions in the Commentary to §1B1.1 (Application Instructions) and the guidelines and commentary in §§1B1.2 through 1B1.8 apply to determinations under this chapter unless otherwise specified. The adjustments in Chapter Three, Parts A (Victim-Related Adjustments), B (Role in the Offense), C (Obstruction), and E (Acceptance of Responsibility) do not apply. The provisions of Chapter Six (Sentencing Procedures, Plea Agreements, and Crime Victims' Rights) apply to proceedings in which the defendant is an organization. Guidelines and policy statements not referenced in this chapter, directly or indirectly, do not apply when the defendant is an organization; e.g., the policy statements in Chapter Seven (Violations of Probation and Supervised Release) do not apply to organizations.

3. The following are definitions of terms used frequently in this chapter:

(A) "Offense" means the offense of conviction and all relevant conduct under §1B1.3 (Relevant Conduct) unless a different meaning is specified or is otherwise clear from the context. The term "instant" is used in connection with "offense," "federal offense," or "offense of conviction," as the case may be, to distinguish the violation for which the defendant is being sentenced from a prior or subsequent offense, or from an offense before another court (e.g., an offense before a state court involving the same underlying conduct).

(B) "High-level personnel of the organization" means individuals who have substantial control over the organization or who have a substantial role in the making of policy within the organization. The term includes: a director; an executive officer; an individual in charge of a major business or functional unit of the organization, such as sales, administration, or finance; and an individual with a substantial ownership interest. "High-level personnel of a unit of the organization" is defined in the Commentary to §8C2.5 (Culpability Score).

(C) "Substantial authority personnel" means individuals who within the scope of their authority exercise a substantial measure of discretion in acting on behalf of an organization. The term includes high-level personnel of the organization, individuals who exercise substantial supervisory authority (e.g., a plant manager, a sales manager), and any other individuals who, although not a part of an organization's management, nevertheless exercise substantial discretion when acting within the scope of their authority (e.g., an individual with authority in an organization to negotiate or set price levels or an individual authorized to negotiate or approve significant contracts). Whether an individual falls within this category must be determined on a case-by-case basis.

(D) "Agent" means any individual, including a director, an officer, an employee, or an independent contractor, authorized to act on behalf of the organization.

(E) An individual "condoned" an offense if the individual knew of the offense and did not take reasonable steps to prevent or terminate the offense.

(F) "Similar misconduct" means prior conduct that is similar in nature to the conduct underlying the instant offense, without regard to whether or not such conduct violated

the same statutory provision. For example, prior Medicare fraud would be misconduct similar to an instant offense involving another type of fraud.

(G) "Prior criminal adjudication" means conviction by trial, plea of guilty (including an Alford plea), or plea of nolo contendere.

(H) "Pecuniary gain" is derived from 18 U.S.C. § 3571(d) and means the additional before-tax profit to the defendant resulting from the relevant conduct of the offense. Gain can result from either additional revenue or cost savings. For example, an offense involving odometer tampering can produce additional revenue. In such a case, the pecuniary gain is the additional revenue received because the automobiles appeared to have less mileage, i.e., the difference between the price received or expected for the automobiles with the apparent mileage and the fair market value of the automobiles with the actual mileage. An offense involving defense procurement fraud related to defective product testing can produce pecuniary gain resulting from cost savings. In such a case, the pecuniary gain is the amount saved because the product was not tested in the required manner.

(I) "Pecuniary loss" is derived from 18 U.S.C. § 3571(d) and is equivalent to the term "loss" as used in Chapter Two (Offense Conduct). See Commentary to §2B1.1 (Theft, Property Destruction, and Fraud), and definitions of "tax loss" in Chapter Two, Part T (Offenses Involving Taxation).

(J) An individual was "willfully ignorant of the offense" if the individual did not investigate the possible occurrence of unlawful conduct despite knowledge of circumstances that would lead a reasonable person to investigate whether unlawful conduct had occurred.

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422); November 1, 1997 (see Appendix C, amendment 546); November 1, 2001 (see Appendix C, amendment 617); November 1, 2004 (see Appendix C, amendment 673); November 1, 2010 (see Appendix C, amendment 747).

PART B - REMEDYING HARM FROM CRIMINAL CONDUCT, AND EFFECTIVE COMPLIANCE AND ETHICS PROGRAM

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422). Amended effective November 1, 2004 (see Appendix C, amendment 673).

1. REMEDYING HARM FROM CRIMINAL CONDUCT

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).

Introductory Commentary

As a general principle, the court should require that the organization take all appropriate steps to provide compensation to victims and otherwise remedy the harm caused or threatened by the offense. A restitution order or an order of probation requiring restitution can be used to compensate identifiable victims of the offense. A remedial order or an order of probation requiring community service can be used to reduce or eliminate the harm threatened, or to repair the harm caused by the offense, when that harm or threatened harm would otherwise not be remedied. An order of notice to victims can be used to notify unidentified victims of the offense.

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422).

§8B1.1. Restitution - Organizations

(a) In the case of an identifiable victim, the court shall --

(1) enter a restitution order for the full amount of the victim's loss, if such order is authorized under 18 U.S.C. § 2248, § 2259, § 2264, § 2327, § 3663, or § 3663A; or

(2) impose a term of probation or supervised release with a condition requiring restitution for the full amount of the victim's loss, if the offense is not an offense for which restitution is authorized under 18 U.S.C. § 3663(a)(1) but otherwise meets the criteria for an order of restitution under that section.

(b) *Provided*, that the provisions of subsection (a) do not apply --

(1) when full restitution has been made; or

(2) in the case of a restitution order under § 3663; a restitution order under 18 U.S.C. § 3663A that pertains to an offense against property described in 18 U.S.C. § 3663A(c)(1)(A)(ii); or a condition of restitution imposed pursuant to subsection (a)(2) above, to the extent the court finds, from facts on the record, that (A) the number of identifiable victims is so large

as to make restitution impracticable; or (B) determining complex issues of fact related to the cause or amount of the victim's losses would complicate or prolong the sentencing process to a degree that the need to provide restitution to any victim is outweighed by the burden on the sentencing process.

(c) If a defendant is ordered to make restitution to an identifiable victim and to pay a fine, the court shall order that any money paid by the defendant shall first be applied to satisfy the order of restitution.

(d) A restitution order may direct the defendant to make a single, lump sum payment, partial payments at specified intervals, in-kind payments, or a combination of payments at specified intervals and in-kind payments. See 18 U.S.C. § 3664(f)(3)(A). An in-kind payment may be in the form of (1) return of property; (2) replacement of property; or (3) if the victim agrees, services rendered to the victim or to a person or organization other than the victim. See 18 U.S.C. § 3664(f)(4).

(e) A restitution order may direct the defendant to make nominal periodic payments if the court finds from facts on the record that the economic circumstances of the defendant do not allow the payment of any amount of a restitution order, and do not allow for the payment of the full amount of a restitution order in the foreseeable future under any reasonable schedule of payments.

(f) Special Instruction

(1) This guideline applies only to a defendant convicted of an offense committed on or after November 1, 1997. Notwithstanding the provisions of §1B1.11 (Use of Guidelines Manual in Effect on Date of Sentencing), use the former §8B1.1 (set forth in Appendix C, amendment 571) in lieu of this guideline in any other case.

Commentary

Background: Section 3553(a)(7) of Title 18, United States Code, requires the court, "in determining the particular sentence to be imposed," to consider "the need to provide restitution to any victims of the offense." Orders of restitution are authorized under 18 U.S.C. §§ 2248, 2259, 2264, 2327, 3663, and 3663A. For offenses for which an order of restitution is not authorized, restitution may be imposed as a condition of probation.

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422); November 1, 1997 (see Appendix C, amendment 571).

§8B1.2. Remedial Orders - Organizations (Policy Statement)

(a) To the extent not addressed under §8B1.1 (Restitution - Organizations), a remedial order imposed as a condition of probation may require the organization to remedy the harm caused by the offense and to eliminate or reduce the risk that

the instant offense will cause future harm.

(b) If the magnitude of expected future harm can be reasonably estimated, the court may require the organization to create a trust fund sufficient to address that expected harm.

Commentary

Background: The purposes of a remedial order are to remedy harm that has already occurred and to prevent future harm. A remedial order requiring corrective action by the organization may be necessary to prevent future injury from the instant offense, e.g., a product recall for a food and drug violation or a clean-up order for an environmental violation. In some cases in which a remedial order potentially may be appropriate, a governmental regulatory agency, e.g., the Environmental Protection Agency or the Food and Drug Administration, may have authority to order remedial measures. In such cases, a remedial order by the court may not be necessary. If a remedial order is entered, it should be coordinated with any administrative or civil actions taken by the appropriate governmental regulatory agency.

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422).

§8B1.3. Community Service - Organizations (Policy Statement)

Community service may be ordered as a condition of probation where such community service is reasonably designed to repair the harm caused by the offense.

Commentary

Background: An organization can perform community service only by employing its resources or paying its employees or others to do so. Consequently, an order that an organization perform community service is essentially an indirect monetary sanction, and therefore generally less desirable than a direct monetary sanction. However, where the convicted organization possesses knowledge, facilities, or skills that uniquely qualify it to repair damage caused by the offense, community service directed at repairing damage may provide an efficient means of remedying harm caused.

In the past, some forms of community service imposed on organizations have not been related to the purposes of sentencing. Requiring a defendant to endow a chair at a university or to contribute to a local charity would not be consistent with this section unless such community service provided a means for preventive or corrective action directly related to the offense and therefore served one of the purposes of sentencing set forth in 18 U.S.C. § 3553(a).

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422).

§8B1.4. Order of Notice to Victims - Organizations

Apply §5F1.4 (Order of Notice to Victims).

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422).

2. EFFECTIVE COMPLIANCE AND ETHICS PROGRAM

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).

§8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (c)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize 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.

(6) The organization's compliance and ethics 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.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

Commentary

Application Notes:

1. *Definitions.—For purposes of this guideline:*

"Compliance and ethics program" means a program designed to prevent and detect criminal conduct.

"Governing authority" means the (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization.

"High-level personnel of the organization" and "substantial authority personnel" have the meaning given those terms in the Commentary to §8A1.2 (Application Instructions - Organizations).

"Standards and procedures" means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct.

2. *Factors to Consider in Meeting Requirements of this Guideline.—*

(A) In General.—Each of the requirements set forth in this guideline shall be met by an organization; however, in determining what specific actions are necessary to meet those requirements, factors that shall be considered include: (i) applicable industry practice or the standards called for by any applicable governmental regulation; (ii) the size of the organization; and (iii) similar misconduct.

(B) Applicable Governmental Regulation and Industry Practice.—An organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.

(C) The Size of the Organization.—

(i) In General.—The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization's standards and procedures, depend on the size of the organization.

(ii) Large Organizations.—A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization. As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.

(iii) Small Organizations.—In meeting the requirements of this guideline, small organizations shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations. However, a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems.

Examples of the informality and use of fewer resources with which a small organization may meet the requirements of this guideline include the following: (I) the governing authority's discharge of its responsibility for oversight of the compliance and ethics program by directly managing the organization's compliance and ethics efforts; (II) training employees through informal staff meetings, and monitoring through regular "walk-arounds" or continuous observation while managing the organization; (III) using available personnel, rather than employing separate staff, to carry out the compliance and ethics program; and (IV) modeling its own compliance and ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.

(D) Recurrence of Similar Misconduct.—Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of this guideline. For purposes of this subparagraph, "similar misconduct" has the meaning given that term in the Commentary to §8A1.2 (Application Instructions - Organizations).

3. Application of Subsection (b)(2).—High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program, shall perform their assigned duties consistent with the exercise of due diligence, and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

If the specific individual(s) assigned overall responsibility for the compliance and ethics program does not have day-to-day operational responsibility for the program, then the individual(s) with day-to-day operational responsibility for the program typically should, no

less than annually, give the governing authority or an appropriate subgroup thereof information on the implementation and effectiveness of the compliance and ethics program.

4. Application of Subsection (b)(3).—

(A) Consistency with Other Law.—Nothing in subsection (b)(3) is intended to require conduct inconsistent with any Federal, State, or local law, including any law governing employment or hiring practices.

(B) Implementation.—In implementing subsection (b)(3), the organization shall hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with the exercise of due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law under subsection (a). With respect to the hiring or promotion of such individuals, an organization shall consider the relatedness of the individual's illegal activities and other misconduct (i.e., other conduct inconsistent with an effective compliance and ethics program) to the specific responsibilities the individual is anticipated to be assigned and other factors such as: (i) the recency of the individual's illegal activities and other misconduct; and (ii) whether the individual has engaged in other such illegal activities and other such misconduct.

5. Application of Subsection (b)(6).—Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

6. Application of Subsection (b)(7).—Subsection (b)(7) has two aspects.

First, the organization should respond appropriately to the criminal conduct. The organization should take reasonable steps, as warranted under the circumstances, to remedy the harm resulting from the criminal conduct. These steps may include, where appropriate, providing restitution to identifiable victims, as well as other forms of remediation. Other reasonable steps to respond appropriately to the criminal conduct may include self-reporting and cooperation with authorities.

Second, the organization should act appropriately to prevent further similar criminal conduct, including assessing the compliance and ethics program and making modifications necessary to ensure the program is effective. The steps taken should be consistent with subsections (b)(5) and (c) and may include the use of an outside professional advisor to ensure adequate assessment and implementation of any modifications.

7. Application of Subsection (c).—To meet the requirements of subsection (c), an organization shall:

(A) Assess periodically the risk that criminal conduct will occur, including assessing the following:

(i) The nature and seriousness of such criminal conduct.

(ii) The likelihood that certain criminal conduct may occur because of the nature of the organization's business. If, because of the nature of an organization's business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct. For example, an organization that, due to the nature of its business, employs sales personnel who have flexibility to set prices shall establish standards and procedures designed to prevent and detect price-fixing. An organization that, due to the nature of its business, employs sales personnel who have flexibility to represent the material characteristics of a product shall establish standards and procedures designed to prevent and detect fraud.

(iii) The prior history of the organization. The prior history of an organization may indicate types of criminal conduct that it shall take actions to prevent and detect.

(B) Prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b), in order to focus on preventing and detecting the criminal conduct identified under subparagraph (A) of this note as most serious, and most likely, to occur.

(C) Modify, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) to reduce the risk of criminal conduct identified under subparagraph (A) of this note as most serious, and most likely, to occur.

Background: This section sets forth the requirements for an effective compliance and ethics program. This section responds to section 805(a)(2)(5) of the Sarbanes-Oxley Act of 2002, Public Law 107–204, which directed the Commission to review and amend, as appropriate, the guidelines and related policy statements to ensure that the guidelines that apply to organizations in this chapter "are sufficient to deter and punish organizational criminal misconduct."

The requirements set forth in this guideline are intended to achieve reasonable prevention and detection of criminal conduct for which the organization would be vicariously liable. The prior diligence of an organization in seeking to prevent and detect criminal conduct has a direct bearing on the appropriate penalties and probation terms for the organization if it is convicted and sentenced for a criminal offense.

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673). Amended effective November 1, 2010 (see Appendix C, amendment 744).

Resource 4

Yates Memo

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

September 9, 2015

MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION
THE ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION
THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
THE ASSISTANT ATTORNEY GENERAL, ENVIRONMENT AND NATURAL RESOURCES DIVISION
THE ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION
THE ASSISTANT ATTORNEY GENERAL, TAX DIVISION
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR, EXECUTIVE OFFICE FOR UNITED STATES TRUSTEES
ALL UNITED STATES ATTORNEYS

FROM: Sally Quillian Yates
Deputy Attorney General

SUBJECT: Individual Accountability for Corporate Wrongdoing

Fighting corporate fraud and other misconduct is a top priority of the Department of Justice. Our nation's economy depends on effective enforcement of the civil and criminal laws that protect our financial system and, by extension, all our citizens. These are principles that the Department lives and breathes—as evidenced by the many attorneys, agents, and support staff who have worked tirelessly on corporate investigations, particularly in the aftermath of the financial crisis.

One of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing. Such accountability is important for several reasons: it deters future illegal activity, it incentivizes changes in corporate behavior, it ensures that the proper parties are held responsible for their actions, and it promotes the public's confidence in our justice system.

There are, however, many substantial challenges unique to pursuing individuals for corporate misdeeds. In large corporations, where responsibility can be diffuse and decisions are made at various levels, it can be difficult to determine if someone possessed the knowledge and criminal intent necessary to establish their guilt beyond a reasonable doubt. This is particularly true when determining the culpability of high-level executives, who may be insulated from the day-to-day activity in which the misconduct occurs. As a result, investigators often must reconstruct what happened based on a painstaking review of corporate documents, which can number in the millions, and which may be difficult to collect due to legal restrictions.

These challenges make it all the more important that the Department fully leverage its resources to identify culpable individuals at all levels in corporate cases. To address these challenges, the Department convened a working group of senior attorneys from Department components and the United States Attorney community with significant experience in this area. The working group examined how the Department approaches corporate investigations, and identified areas in which it can amend its policies and practices in order to most effectively pursue the individuals responsible for corporate wrongs. This memo is a product of the working group's discussions.

The measures described in this memo are steps that should be taken in any investigation of corporate misconduct. Some of these measures are new, while others reflect best practices that are already employed by many federal prosecutors. Fundamentally, this memo is designed to ensure that all attorneys across the Department are consistent in our best efforts to hold to account the individuals responsible for illegal corporate conduct.

The guidance in this memo will also apply to civil corporate matters. In addition to recovering assets, civil enforcement actions serve to redress misconduct and deter future wrongdoing. Thus, civil attorneys investigating corporate wrongdoing should maintain a focus on the responsible individuals, recognizing that holding them to account is an important part of protecting the public fisc in the long term.

The guidance in this memo reflects six key steps to strengthen our pursuit of individual corporate wrongdoing, some of which reflect policy shifts and each of which is described in greater detail below: (1) in order to qualify for any cooperation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct; (2) criminal and civil corporate investigations should focus on individuals from the inception of the investigation; (3) criminal and civil attorneys handling corporate investigations should be in routine communication with one another; (4) absent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation; (5) Department attorneys should not resolve matters with a corporation without a clear plan to resolve related individual cases, and should

memorialize any declinations as to individuals in such cases; and (6) civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.[1]

I have directed that certain criminal and civil provisions in the United States Attorney's Manual, more specifically the Principles of Federal Prosecution of Business Organizations (USAM 9-28.000 *et seq.*) and the commercial litigation provisions in Title 4 (USAM 4-4.000 *et seq.*), be revised to reflect these changes. The guidance in this memo will apply to all future investigations of corporate wrongdoing. It will also apply to those matters pending as of the date of this memo, to the extent it is practicable to do so.

1. To be eligible for <u>any</u> cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct.

In order for a company to receive <u>any</u> consideration for cooperation under the Principles of Federal Prosecution of Business Organizations, the company must completely disclose to the Department all relevant facts about individual misconduct. Companies cannot pick and choose what facts to disclose. That is, to be eligible for any credit for cooperation, the company must identify all individuals involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide to the Department all facts relating to that misconduct. If a company seeking cooperation credit declines to learn of such facts or to provide the Department with complete factual information about individual wrongdoers, its cooperation will not be considered a mitigating factor pursuant to USAM 9-28.700 *et seq.*[2] Once a company meets the threshold requirement of providing all relevant facts with respect to individuals, it will be eligible for consideration for cooperation credit. The extent of that cooperation credit will depend on all the various factors that have traditionally applied in making this assessment (*e.g.*, the timeliness of the cooperation, the diligence, thoroughness, and speed of the internal investigation, the proactive nature of the cooperation, etc.).

This condition of cooperation applies equally to corporations seeking to cooperate in civil matters; a company under civil investigation must provide to the Department all relevant facts about individual misconduct in order to receive any consideration in the negotiation. For

---

[1] The measures laid out in this memo are intended solely to guide attorneys for the government in accordance with their statutory responsibilities and federal law. They are not intended to, do not, and may not be relied upon to create a right or benefit, substantive or procedural, enforceable at law by a party to litigation with the United States.

[2] Nor, if a company is prosecuted, will it support a cooperation-related reduction at sentencing. *See* U.S.S.G. USSG § 8C2.5(g), Application Note 13 ("A prime test of whether the organization has disclosed all pertinent information" necessary to receive a cooperation-related reduction in its offense level calculation "is whether the information is sufficient ... to identify ... the individual(s) responsible for the criminal conduct").

example, the Department's position on "full cooperation" under the False Claims Act, 31 U.S.C. § 3729(a)(2), will be that, at a minimum, all relevant facts about responsible individuals must be provided.

The requirement that companies cooperate completely as to individuals, within the bounds of the law and legal privileges, *see* USAM 9-28.700 to 9-28.760, does not mean that Department attorneys should wait for the company to deliver the information about individual wrongdoers and then merely accept what companies provide. To the contrary, Department attorneys should be proactively investigating individuals at every step of the process – before, during, and after any corporate cooperation. Department attorneys should vigorously review any information provided by companies and compare it to the results of their own investigation, in order to best ensure that the information provided is indeed complete and does not seek to minimize the behavior or role of any individual or group of individuals.

Department attorneys should strive to obtain from the company as much information as possible about responsible individuals before resolving the corporate case. But there may be instances where the company's continued cooperation with respect to individuals will be necessary post-resolution. In these circumstances, the plea or settlement agreement should include a provision that requires the company to provide information about all culpable individuals and that is explicit enough so that a failure to provide the information results in specific consequences, such as stipulated penalties and/or a material breach.

2. Both criminal and civil corporate investigations should focus on individuals from the inception of the investigation.

Both criminal and civil attorneys should focus on individual wrongdoing from the very beginning of any investigation of corporate misconduct. By focusing on building cases against individual wrongdoers from the inception of an investigation, we accomplish multiple goals. First, we maximize our ability to ferret out the full extent of corporate misconduct. Because a corporation only acts through individuals, investigating the conduct of individuals is the most efficient and effective way to determine the facts and extent of any corporate misconduct. Second, by focusing our investigation on individuals, we can increase the likelihood that individuals with knowledge of the corporate misconduct will cooperate with the investigation and provide information against individuals higher up the corporate hierarchy. Third, by focusing on individuals from the very beginning of an investigation, we maximize the chances that the final resolution of an investigation uncovering the misconduct will include civil or criminal charges against not just the corporation but against culpable individuals as well.

3. Criminal and civil attorneys handling corporate investigations should be in routine communication with one another.

Early and regular communication between civil attorneys and criminal prosecutors handling corporate investigations can be crucial to our ability to effectively pursue individuals in

these matters. Consultation between the Department's civil and criminal attorneys, together with agency attorneys, permits consideration of the full range of the government's potential remedies (including incarceration, fines, penalties, damages, restitution to victims, asset seizure, civil and criminal forfeiture, and exclusion, suspension and debarment) and promotes the most thorough and appropriate resolution in every case. That is why the Department has long recognized the importance of parallel development of civil and criminal proceedings. *See* USAM 1-12.000.

Criminal attorneys handling corporate investigations should notify civil attorneys as early as permissible of conduct that might give rise to potential individual civil liability, even if criminal liability continues to be sought. Further, if there is a decision not to pursue a criminal action against an individual – due to questions of intent or burden of proof, for example – criminal attorneys should confer with their civil counterparts so that they may make an assessment under applicable civil statutes and consistent with this guidance. Likewise, if civil attorneys believe that an individual identified in the course of their corporate investigation should be subject to a criminal inquiry, that matter should promptly be referred to criminal prosecutors, regardless of the current status of the civil corporate investigation.

Department attorneys should be alert for circumstances where concurrent criminal and civil investigations of individual misconduct should be pursued. Coordination in this regard should happen early, even if it is not certain that a civil or criminal disposition will be the end result for the individuals or the company.

4. Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals.

There may be instances where the Department reaches a resolution with the company before resolving matters with responsible individuals. In these circumstances, Department attorneys should take care to preserve the ability to pursue these individuals. Because of the importance of holding responsible individuals to account, absent extraordinary circumstances or approved departmental policy such as the Antitrust Division's Corporate Leniency Policy, Department lawyers should not agree to a corporate resolution that includes an agreement to dismiss charges against, or provide immunity for, individual officers or employees. The same principle holds true in civil corporate matters; absent extraordinary circumstances, the United States should not release claims related to the liability of individuals based on corporate settlement releases. Any such release of criminal or civil liability due to extraordinary circumstances must be personally approved in writing by the relevant Assistant Attorney General or United States Attorney.

5. **Corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires and declinations as to individuals in such cases must be memorialized.**

If the investigation of individual misconduct has not concluded by the time authorization is sought to resolve the case against the corporation, the prosecution or corporate authorization memorandum should include a discussion of the potentially liable individuals, a description of the current status of the investigation regarding their conduct and the investigative work that remains to be done, and an investigative plan to bring the matter to resolution prior to the end of any statute of limitations period. If a decision is made at the conclusion of the investigation not to bring civil claims or criminal charges against the individuals who committed the misconduct, the reasons for that determination must be memorialized and approved by the United States Attorney or Assistant Attorney General whose office handled the investigation, or their designees.

Delays in the corporate investigation should not affect the Department's ability to pursue potentially culpable individuals. While every effort should be made to resolve a corporate matter within the statutorily allotted time, and tolling agreements should be the rare exception, in situations where it is anticipated that a tolling agreement is nevertheless unavoidable and necessary, all efforts should be made either to resolve the matter against culpable individuals before the limitations period expires or to preserve the ability to charge individuals by tolling the limitations period by agreement or court order.

6. **Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.**

The Department's civil enforcement efforts are designed not only to return government money to the public fisc, but also to hold the wrongdoers accountable and to deter future wrongdoing. These twin aims – of recovering as much money as possible, on the one hand, and of accountability for and deterrence of individual misconduct, on the other – are equally important. In certain circumstances, though, these dual goals can be in apparent tension with one another, for example, when it comes to the question of whether to pursue civil actions against individual corporate wrongdoers who may not have the necessary financial resources to pay a significant judgment.

Pursuit of civil actions against culpable individuals should not be governed solely by those individuals' ability to pay. In other words, the fact that an individual may not have sufficient resources to satisfy a significant judgment should not control the decision on whether to bring suit. Rather, in deciding whether to file a civil action against an individual, Department attorneys should consider factors such as whether the person's misconduct was serious, whether

it is actionable, whether the admissible evidence will probably be sufficient to obtain and sustain a judgment, and whether pursuing the action reflects an important federal interest. Just as our prosecutors do when making charging decisions, civil attorneys should make individualized assessments in deciding whether to bring a case, taking into account numerous factors, such as the individual's misconduct and past history and the circumstances relating to the commission of the misconduct, the needs of the communities we serve, and federal resources and priorities.

Although in the short term certain cases against individuals may not provide as robust a monetary return on the Department's investment, pursuing individual actions in civil corporate matters will result in significant long-term deterrence. Only by seeking to hold individuals accountable in view of all of the factors above can the Department ensure that it is doing everything in its power to minimize corporate fraud, and, over the course of time, minimize losses to the public fisc through fraud.

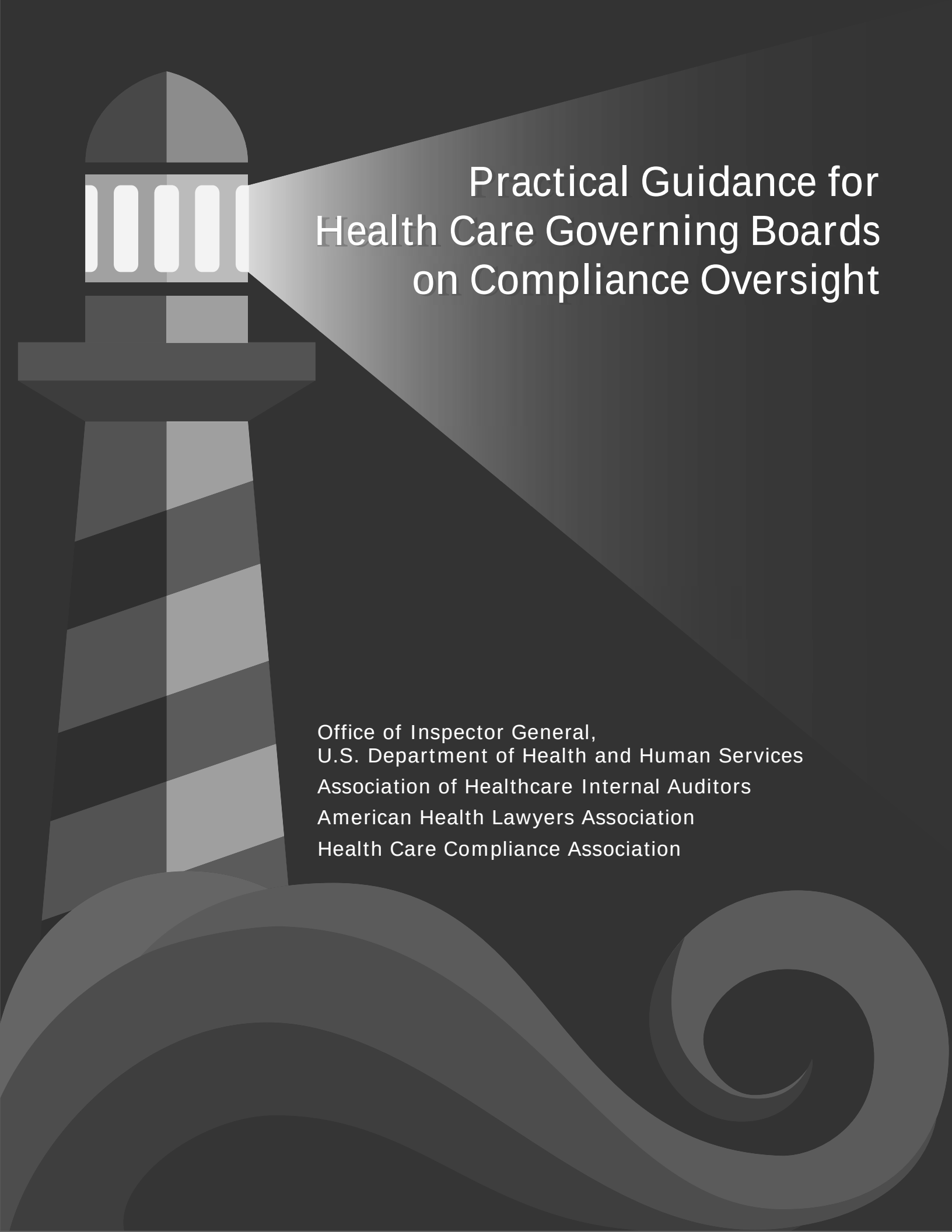
Conclusion

The Department makes these changes recognizing the challenges they may present. But we are making these changes because we believe they will maximize our ability to deter misconduct and to hold those who engage in it accountable.

In the months ahead, the Department will be working with components to turn these policies into everyday practice. On September 16, 2015, for example, the Department will be hosting a training conference in Washington, D.C., on this subject, and I look forward to further addressing the topic with some of you then.

Resource 5

Practical Guidance for Health Care Governing Boards on Compliance Oversight



Practical Guidance for Health Care Governing Boards on Compliance Oversight

Office of Inspector General,
U.S. Department of Health and Human Services
Association of Healthcare Internal Auditors
American Health Lawyers Association
Health Care Compliance Association

About the Organizations

This educational resource was developed in collaboration between the Association of Healthcare Internal Auditors (AHIA), the American Health Lawyers Association (AHLA), the Health Care Compliance Association (HCCA), and the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS).

AHIA is an international organization dedicated to the advancement of the health care internal auditing profession. The AHLA is the Nation's largest nonpartisan, educational organization devoted to legal issues in the health care field. HCCA is a member-based, nonprofit organization serving compliance professionals throughout the health care field. OIG's mission is to protect the integrity of more than 100 HHS programs, including Medicare and Medicaid, as well as the health and welfare of program beneficiaries.

The following individuals, representing these organizations, served on the drafting task force for this document:

Katherine Matos, Senior Counsel, OIG, HHS

Felicia E. Heimer, Senior Counsel, OIG, HHS

Catherine A. Martin, Principal, Ober | Kaler (AHLA)

Robert R. Michalski, Chief Compliance Officer, Baylor Scott & White Health (AHIA)

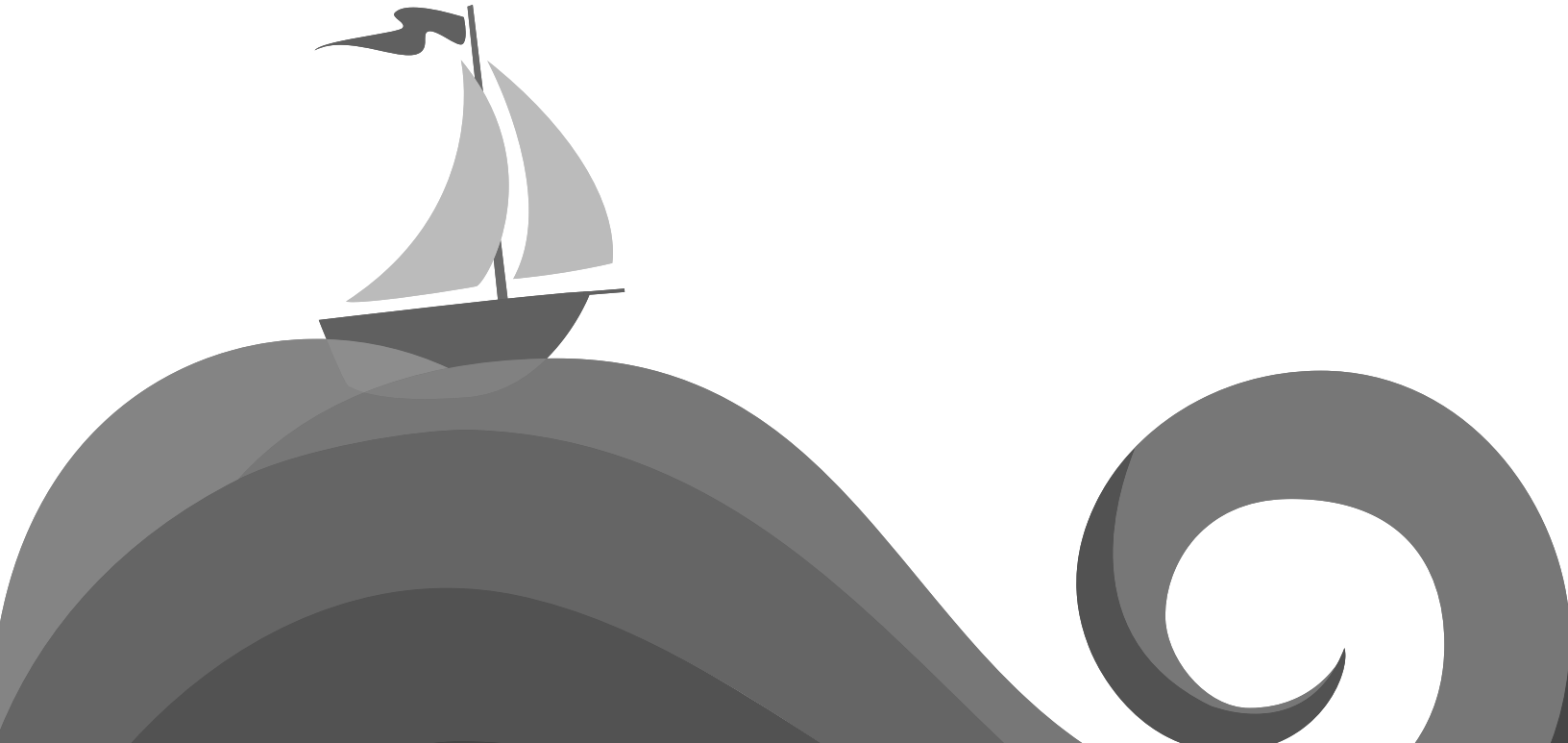
Daniel Roach, General Counsel and Chief Compliance Officer, Optum360 (HCCA)

Sanford V. Teplitzky, Principal, Ober | Kaler (AHLA)

Published on April 20, 2015.

This document is intended to assist governing boards of health care organizations (Boards) to responsibly carry out their compliance plan oversight obligations under applicable laws. This document is intended as guidance and should not be interpreted as setting any particular standards of conduct. The authors recognize that each health care entity can, and should, take the necessary steps to ensure compliance with applicable Federal, State, and local law. At the same time, the authors also recognize that there is no uniform approach to compliance. No part of this document should be taken as the opinion of, or as legal or professional advice from, any of the authors or their respective agencies or organizations.

Table of Contents



Introduction

Previous guidance[1] has consistently emphasized the need for Boards to be fully engaged in their oversight responsibility. A critical element of effective oversight is the process of asking the right questions of management to determine the adequacy and effectiveness of the organization's compliance program, as well as the performance of those who develop and execute that program, and to make compliance a responsibility for all levels of management. Given heightened industry and professional interest in governance and transparency issues, this document seeks to provide practical tips for Boards as they work to effectuate their oversight role of their organizations' compliance with State and Federal laws that regulate the health care industry. Specifically, this document addresses issues relating to a Board's oversight and review of compliance program functions, including the: (1) roles of, and relationships between, the organization's audit, compliance, and legal departments; (2) mechanism and process for issue-reporting within an organization; (3) approach to identifying regulatory risk; and (4) methods of encouraging enterprise-wide accountability for achievement of compliance goals and objectives.

A critical element of effective oversight is the process of asking the right questions....

1 OIG and AHLA, *Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors* (2003); OIG and AHLA, *An Integrated Approach to Corporate Compliance: A Resource for Health Care Organization Boards of Directors* (2004); and OIG and AHLA, *Corporate Responsibility and Health Care Quality: A Resource for Health Care Boards of Directors* (2007).

Expectations for Board Oversight of Compliance Program Functions

A Board must act in good faith in the exercise of its oversight responsibility for its organization, including making inquiries to ensure: (1) a corporate information and reporting system exists and (2) the reporting system is adequate to assure the Board that appropriate information relating to compliance with applicable laws will come to its attention timely and as a matter of course.[2] The existence of a corporate reporting system is a key compliance program element, which not only keeps the Board informed of the activities of the organization, but also enables an organization to evaluate and respond to issues of potentially illegal or otherwise inappropriate activity.

Boards are encouraged to use widely recognized public compliance resources as benchmarks for their organizations. The Federal Sentencing Guidelines (Guidelines),[3] OIG's voluntary compliance program guidance documents,[4] and OIG Corporate Integrity Agreements (CIAs) can be used as baseline assessment tools for Boards and management in determining what specific functions may be necessary to meet the requirements of an effective compliance program. The Guidelines "offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program."[5] The compliance program guidance documents were developed by OIG to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements. CIAs impose specific structural and reporting requirements to

---

2 *In re Caremark Int'l, Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

3 U.S. Sentencing Commission, *Guidelines Manual* (Nov. 2013) (USSG), http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2013/manual-pdf/2013_Guidelines_Manual_Full.pdf.

4 OIG, *Compliance Guidance*, http://oig.hhs.gov/compliance/compliance-guidance/index.asp.

5 USSG Ch. 8, Intro. Comment.

promote compliance with Federal health care program standards at entities that have resolved fraud allegations.

Basic CIA elements mirror those in the Guidelines, but a CIA also includes obligations tailored to the organization and its compliance risks. Existing CIAs may be helpful resources for Boards seeking to evaluate their organizations' compliance programs. OIG has required some settling entities, such as health systems and hospitals, to agree to Board-level requirements, including annual resolutions. These resolutions are signed by each member of the Board, or the designated Board committee, and detail the activities that have been undertaken to review and oversee the organization's compliance with Federal health care program and CIA requirements. OIG has not required this level of Board involvement in every case, but these provisions demonstrate the importance placed on Board oversight in cases OIG believes reflect serious compliance failures.

Although compliance program design is not a "one size fits all" issue, Boards are expected to put forth a meaningful effort....

Although compliance program design is not a "one size fits all" issue, Boards are expected to put forth a meaningful effort to review the adequacy of existing compliance systems and functions. Ensuring that management is aware of the Guidelines, compliance program guidance, and relevant CIAs is a good first step.

One area of inquiry for Board members of health care organizations should be the scope and adequacy of the compliance program in light of the size and complexity of their organizations. The Guidelines allow for variation according to "the size of the organization."[6] In accordance with the Guidelines,

6 USSG § 8B2.1, comment. (n. 2).

OIG recognizes that the design of a compliance program will depend on the size and resources of the organization.[7] Additionally, the complexity of the organization will likely dictate the nature and magnitude of regulatory impact and thereby the nature and skill set of resources needed to manage and monitor compliance.

While smaller or less complex organizations must demonstrate the same degree of commitment to ethical conduct and compliance as larger organizations, the Government recognizes that they may meet the Guidelines requirements with less formality and fewer resources than would be expected of larger and more complex organizations.[8] Smaller organizations may meet their compliance responsibility by "using available personnel, rather than employing separate staff, to carry out the compliance and ethics program." Board members of such organizations may wish to evaluate whether the organization is "modeling its own compliance and ethics programs on existing, well-regarded compliance and ethics programs and best practices of other similar organizations."[9] The Guidelines also foresee that Boards of smaller organizations may need to become more involved in the organizations' compliance and ethics efforts than their larger counterparts.[10]

Boards should develop a formal plan to stay abreast of the ever-changing regulatory landscape and operating environment. The plan may involve periodic updates from informed staff or review of regulatory resources made available to them by staff. With an understanding of the dynamic regulatory environment, Boards will be in a position to ask more pertinent questions of management

---

7 Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. 59434, 59436 (Oct. 5, 2000) ("The extent of implementation [of the seven components of a voluntary compliance program] will depend on the size and resources of the practice. Smaller physician practices may incorporate each of the components in a manner that best suits the practice. By contrast, larger physician practices often have the means to incorporate the components in a more systematic manner."); Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289 (Mar. 16, 2000) (recognizing that smaller providers may not be able to outsource their screening process or afford to maintain a telephone hotline).

8 USSG § 8B2.1, comment. (n. 2).

9 *Id.*

10 *Id.*

and make informed strategic decisions regarding the organizations' compliance programs, including matters that relate to funding and resource allocation. For instance, new standards and reporting requirements, as required by law, may, but do not necessarily, result in increased compliance costs for an organization. Board members may also wish to take advantage of outside educational programs that provide them with opportunities to develop a better understanding of industry risks, regulatory requirements, and how effective compliance and ethics programs operate. In addition, Boards may want management to create a formal education calendar that ensures that Board members are periodically educated on the organizations' highest risks.

Finally, a Board can raise its level of substantive expertise with respect to regulatory and compliance matters by adding to the Board, or periodically consulting with, an experienced regulatory, compliance, or legal professional. The presence of a professional with health care compliance expertise on the Board sends a strong message about the organization's commitment to compliance, provides a valuable resource to other Board members, and helps the Board better fulfill its oversight obligations. Board members are generally entitled to rely on the advice of experts in fulfilling their duties.[11] OIG sometimes requires entities under a CIA to retain an expert in compliance or governance issues to assist the Board in fulfilling its responsibilities under the CIA.[12] Experts can assist Boards and management in a variety of ways, including the identification of risk areas, provision of insight into best practices in governance, or consultation on other substantive or investigative matters.

---

11 *See* Del Code Ann. tit. 8, § 141(e) (2010); ABA Revised Model Business Corporation Act, §§ 8.30(e), (f)(2) Standards of Conduct for Directors.

12 *See* Corporate Integrity Agreements between OIG and Halifax Hospital Medical Center and Halifax Staffing, Inc. (2014, compliance and governance); Johnson & Johnson (2013); Dallas County Hospital District d/b/a Parkland Health and Hospital System (2013, compliance and governance); Forest Laboratories, Inc. (2010); Novartis Pharmaceuticals Corporation (2010); Ortho-McNeil-Janssen Pharmaceuticals, Inc. (2010); Synthes, Inc. (2010, compliance expert retained by Audit Committee); The University of Medicine and Dentistry of New Jersey (2009, compliance expert retained by Audit Committee); Quest Diagnostics Incorporated (2009); Amerigroup Corporation (2008); Bayer HealthCare LLC (2008); and Tenet Healthcare Corporation (2006; retained by the Quality, Compliance, and Ethics Committee of the Board).

Roles and Relationships

Organizations should define the interrelationship of the audit, compliance, and legal functions in charters or other organizational documents. The structure, reporting relationships, and interaction of these and other functions (e.g., quality, risk management, and human resources) should be included as departmental roles and responsibilities are defined. One approach is for the charters to draw functional boundaries while also setting an expectation of cooperation and collaboration among those functions. One illustration is the following, recognizing that not all entities may possess sufficient resources to support this structure:

The compliance function promotes the prevention, detection, and resolution of actions that do not conform to legal, policy, or business standards. This responsibility includes the obligation to develop policies and procedures that provide employees guidance, the creation of incentives to promote employee compliance, the development of plans to improve or sustain compliance, the development of metrics to measure execution (particularly by management) of the program and implementation of corrective actions, and the development of reports and dashboards that help management and the Board evaluate the effectiveness of the program.

The legal function advises the organization on the legal and regulatory risks of its business strategies, providing advice and counsel to management and the Board about relevant laws and regulations that govern, relate to, or impact the organization. The function also defends the organization in legal proceedings and initiates legal proceedings against other parties if such action is warranted.

The internal audit function provides an objective evaluation of the existing risk and internal control systems and framework within an organization. Internal audits ensure monitoring functions are working as intended and identify where management monitoring and/or additional

Board oversight may be required. Internal audit helps management (and the compliance function) develop actions to enhance internal controls, reduce risk to the organization, and promote more effective and efficient use of resources. Internal audit can fulfill the auditing requirements of the Guidelines.

The human resources function manages the recruiting, screening, and hiring of employees; coordinates employee benefits; and provides employee training and development opportunities.

The quality improvement function promotes consistent, safe, and high quality practices within health care organizations. This function improves efficiency and health outcomes by measuring and reporting on quality outcomes and recommends necessary changes to clinical processes to management and the Board. Quality improvement is critical to maintaining patient-centered care and helping the organization minimize risk of patient harm.

Boards should be aware of, and evaluate, the adequacy, independence,[13] and performance of different functions within an organization on a periodic basis. OIG believes an organization's Compliance Officer should neither be counsel for the provider, nor be subordinate in function or position to counsel or the legal department, in any manner.[14] While independent, an organization's counsel and compliance officer should collaborate to further the interests of the organization. OIG's position on separate compliance and legal functions reflects the independent roles and professional obligations of each function;[15]

---

13 Evaluation of independence typically includes assessing whether the function has uninhibited access to the relevant Board committees, is free from organizational bias through an appropriate administrative reporting relationship, and receives fair compensation adjustments based on input from any relevant Board committee.

14 *See* OIG and AHLA, *An Integrated Approach to Corporate Compliance: A Resource for Health Care Organization Boards of Directors*, 3 (2004) (citing Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,997 (Feb. 23, 1998)).

15 *See, generally, id.*

the same is true for internal audit.[16] To operate effectively, the compliance, legal, and internal audit functions should have access to appropriate and relevant corporate information and resources. As part of this effort, organizations will need to balance any existing attorney-client privilege with the goal of providing such access to key individuals who are charged with the responsibility for ensuring compliance, as well as properly reporting and remediating any violations of civil, criminal, or administrative law.

The Board should have a process to ensure appropriate access to information; this process may be set forth in a formal charter document approved by the Audit Committee of the Board or in other appropriate documents. Organizations that do not separate these functions (and some organizations may not have the resources to make this complete separation) should recognize the potential risks of such an arrangement. To partially mitigate these potential risks, organizations should provide individuals serving in multiple roles the capability to execute each function in an independent manner when necessary, including through reporting opportunities with the Board and executive management.

Boards should also evaluate and discuss how management works together to address risk, including the role of each in:

1. identifying compliance risks,
2. investigating compliance risks and avoiding duplication of effort,
3. identifying and implementing appropriate corrective actions and decision-making, and
4. communicating between the various functions throughout the process.

16 Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,997 (Feb. 23, 1998) (auditing and monitoring function should "[b]e independent of physicians and line management"); Compliance Program Guidance for Home Health Agencies, 63 Fed. Reg. 42,410, 42,424 (Aug. 7, 1998) (auditing and monitoring function should "[b]e objective and independent of line management to the extent reasonably possible"); Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289, 14,302 (Mar. 16, 2000).

Boards should understand how management approaches conflicts or disagreements with respect to the resolution of compliance issues and how it decides on the appropriate course of action. The audit, compliance, and legal functions should speak a common language, at least to the Board and management, with respect to governance concepts, such as accountability, risk, compliance, auditing, and monitoring. Agreeing on the adoption of certain frameworks and definitions can help to develop such a common language.

Reporting to the Board

The Board should set and enforce expectations for receiving particular types of compliance-related information from various members of management. The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts—separately and independently—from a variety of key players, including those responsible for audit, compliance, human resources, legal, quality, and information technology. By engaging the leadership team and others deeper in the organization, the Board can identify who can provide relevant information about operations and operational risks. It may be helpful and productive for the Board to establish clear expectations for members of the management team and to hold them accountable for performing and informing the Board in accordance with those expectations. The Board may request the development of objective scorecards that measure how well management is executing the compliance program, mitigating risks, and implementing corrective action plans. Expectations could also include reporting information on internal and external investigations, serious issues raised in internal and external audits, hotline call activity, all allegations of material fraud or senior management misconduct, and all management exceptions to the organization's

The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts....

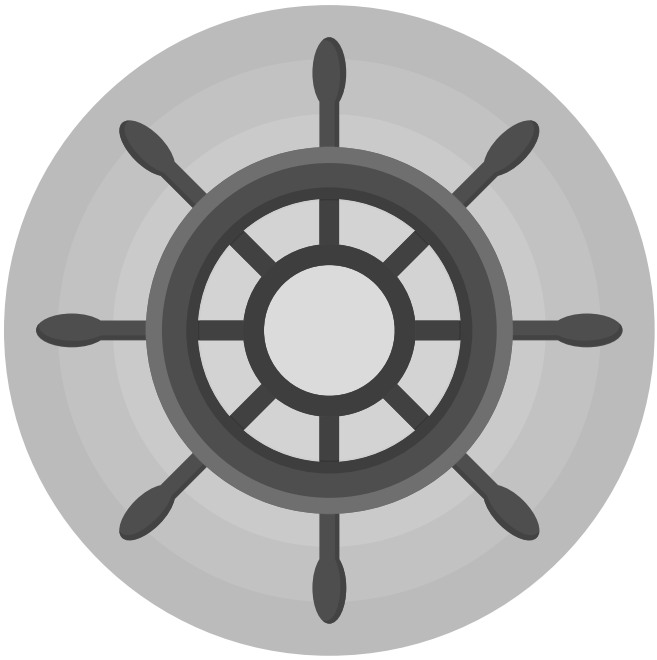
code of conduct and/or expense reimbursement policy. In addition, the Board should expect that management will address significant regulatory changes and enforcement events relevant to the organization's business.

Boards of health care organizations should receive compliance and risk-related information in a format sufficient to satisfy the interests or concerns of their members and to fit their capacity to review that information. Some Boards use tools such as dashboards—containing key financial, operational and compliance indicators to assess risk, performance against budgets, strategic plans, policies and procedures, or other goals and objectives—in order to strike a balance between too much and too little information. For instance, Board quality committees can work with management to create the content of the dashboards with a goal of identifying and responding to risks and improving quality of care. Boards should also consider establishing a risk-based reporting system, in which those responsible for the compliance function provide reports to the Board when certain risk-based criteria are met. The Board should be assured that there are mechanisms in place to ensure timely reporting of suspected violations and to evaluate and implement remedial measures. These tools may also be used to track and identify trends in organizational performance against corrective action plans developed in response to compliance concerns. Regular internal reviews that provide a Board with a snapshot of where the organization is, and where it may be going, in terms of compliance and quality improvement, should produce better compliance results and higher quality services.

As part of its oversight responsibilities, the Board may want to consider conducting regular "executive sessions" (i.e., excluding senior management) with leadership from the compliance, legal, internal audit, and quality functions to encourage more open communication. Scheduling regular executive sessions creates a continuous expectation of open dialogue, rather than calling such a session only when a problem arises, and is helpful to avoid suspicion among management about why a special executive session is being called.

Identifying and Auditing Potential Risk Areas

Some regulatory risk areas are common to all health care providers. Compliance in health care requires monitoring of activities that are highly vulnerable to fraud or other violations. Areas of particular interest include referral relationships and arrangements, billing problems (e.g., upcoding, submitting claims for services not rendered and/or medically unnecessary services), privacy breaches, and quality-related events.



The Board should ensure that management and the Board have strong processes for identifying risk areas. Risk areas may be identified from internal or external information sources. For instance, Boards and management may identify regulatory risks from internal sources, such as employee reports to an internal compliance hotline or internal audits. External sources that may be used to identify regulatory risks might include professional organization publications, OIG-issued guidance, consultants, competitors, or news media. When failures or problems in similar organizations are publicized, Board members should ask their own management teams whether there are controls and processes in place to reduce the risk of, and to identify, similar misconduct or issues within their organizations.

The Board should ensure that management consistently reviews and audits risk areas, as well as develops, implements, and monitors corrective action plans. One of the reasonable steps an organization is expected to take

under the Guidelines is "monitoring and auditing to detect criminal conduct."[17] Audits can pinpoint potential risk factors, identify regulatory or compliance problems, or confirm the effectiveness of compliance controls. Audit results that reflect compliance issues or control deficiencies should be accompanied by corrective action plans.[18]

Recent industry trends should also be considered when designing risk assessment plans. Compliance functions tasked with monitoring new areas of risk should take into account the increasing emphasis on quality, industry consolidation, and changes in insurance coverage and reimbursement. New forms of reimbursement (e.g., value-based purchasing, bundling of services for a single payment, and global payments for maintaining and improving the health of individual patients and even entire populations) lead to new incentives and compliance risks. Payment policies that align payment with quality care have placed increasing pressure to conform to recommended quality guidelines and improve quality outcomes. New payment models have also incentivized consolidation among health care providers and more employment and contractual relationships (e.g., between hospitals and physicians). In light of the fact that statutes applicable to provider-physician relationships are very broad, Boards of entities that have financial relationships with referral sources or recipients should ask how their organizations are reviewing these arrangements for compliance with the physician self-referral (Stark) and anti-kickback laws. There should also be a clear understanding between the Board and management as to how the entity will approach and implement those relationships and what level of risk is acceptable in such arrangements.

Emerging trends in the health care industry to increase transparency can present health care organizations with opportunities and risks. For example, the Government is collecting and publishing data on health outcomes and quality measures (e.g., Centers for Medicare & Medicaid Services (CMS) Quality Compare Measures), Medicare payment data are now publicly available (e.g.,

---

17 *See* USSG § 8B2.1(b)(5).

18 *See* USSG § 8B2.1(c).

CMS physician payment data), and the Sunshine Rule[19] offers public access to data on payments from the pharmaceutical and device industries to physicians. Boards should consider all beneficial use of this newly available information. For example, Boards may choose to compare accessible data against organizational peers and incorporate national benchmarks when assessing organizational risk and compliance. Also, Boards of organizations that employ physicians should be cognizant of the relationships that exist between their employees and other health care entities and whether those relationships could have an impact on such matters as clinical and research decision-making. Because so much more information is becoming public, Boards may be asked significant compliance-oriented questions by various stakeholders, including patients, employees, government officials, donors, the media, and whistleblowers.

Encouraging Accountability and Compliance

Compliance is an enterprise-wide responsibility. While audit, compliance, and legal functions serve as advisors, evaluators, identifiers, and monitors of risk and compliance, it is the responsibility of the entire organization to execute the compliance program.

Compliance is an enterprise-wide responsiblity.

In an effort to support the concept that compliance is "a way of life," a Board may assess employee performance in promoting and adhering to compliance.[20] An organization may assess individual, department, or facility-level performance or consistency in executing the compliance program. These assessments can then be used to either withhold incentives or to provide bonuses

---

19 *See* Sunshine Rule, 42 C.F.R. § 403.904, and CMS *Open Payments*, http://www.cms.gov/Regulations-and-Guidance/Legislation/National-Physician-Payment-Transparency-Program/index.html.

20 Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289, 14,298-14,299 (Mar. 16, 2000).

based on compliance and quality outcomes. Some companies have made participation in annual incentive programs contingent on satisfactorily meeting annual compliance goals. Others have instituted employee and executive compensation claw-back/recoupment provisions if compliance metrics are not met. Such approaches mirror Government trends. For example, OIG is increasingly requiring certifications of compliance from managers outside the compliance department. Through a system of defined compliance goals and objectives against which performance may be measured and incentivized, organizations can effectively communicate the message that everyone is ultimately responsible for compliance.

Governing Boards have multiple incentives to build compliance programs that encourage self-identification of compliance failures and to voluntarily disclose such failures to the Government. For instance, providers enrolled in Medicare or Medicaid are required by statute to report and refund any overpayments under what is called the 60 Day Rule.[21] The 60-Day Rule requires all Medicare and Medicaid participating providers and suppliers to report and refund known overpayments within 60 days from the date the overpayment is "identified" or within 60 days of the date when any corresponding cost report is due. Failure to follow the 60-Day Rule can result in False Claims Act or civil monetary penalty liability. The final regulations, when released, should provide additional guidance and clarity as to what it means to "identify" an overpayment.[22] However, as an example, a Board would be well served by asking management about its efforts to develop policies for identifying and returning overpayments. Such an inquiry would inform the Board about how proactive the organization's compliance program may be in correcting and remediating compliance issues.

---

21 42 U.S.C. § 1320a-7k.

22 Medicare Program; Reporting and Returning of Overpayments, 77 Fed. Reg. 9179, 9182 (Feb. 16, 2012) (Under the proposed regulations interpreting this statutory requirement, an overpayment is "identified" when a person "has actual knowledge of the existence of the overpayment or acts in reckless disregard or deliberate ignorance of the overpayment.") disregard or deliberate ignorance of the overpayment."); Medicare Program; Reporting and Returning of Overpayments; Extensions of Timeline for Publication of the Final Rule, 80 Fed. Reg. 8247 (Feb. 17, 2015).

Organizations that discover a violation of law often engage in an internal analysis of the benefits and costs of disclosing—and risks of failing to disclose—such violation to OIG and/or another governmental agency. Organizations that are proactive in self-disclosing issues under OIG's Self-Disclosure Protocol realize certain benefits, such as (1) faster resolution of the case—the average OIG self-disclosure is resolved in less than one year; (2) lower payment—OIG settles most self-disclosure cases for 1.5 times damages rather than for double or treble damages and penalties available under the False Claims Act; and (3) exclusion release as part of settlement with no CIA or other compliance obligations.[23] OIG believes that providers have legal and ethical obligations to disclose known violations of law occurring within their organizations.[24] Boards should ask management how it handles the identification of probable violations of law, including voluntary self-disclosure of such issues to the Government.

As an extension of their oversight of reporting mechanisms and structures, Boards would also be well served by evaluating whether compliance systems and processes encourage effective communication across the organizations and whether employees feel confident that raising compliance concerns, questions, or complaints will result in meaningful inquiry without retaliation or retribution. Further, the Board should request and receive sufficient information to evaluate the appropriateness of management's responses to identified violations of the organization's policies or Federal or State laws.

Conclusion

A health care governing Board should make efforts to increase its knowledge of relevant and emerging regulatory risks, the role and functioning of the organization's compliance program in the face of those risks, and the flow and elevation of reporting of potential issues and problems to

---

23 *See* OIG, *Self-Disclosure Information*, http://oig.hhs.gov/compliance/self-disclosure-info.

24 *See id.*, at 2 ("we believe that using the [Self-Disclosure Protocol] may mitigate potential exposure under section 1128J(d) of the Act, 42 U.S.C. 1320a-7k(d).")

senior management. A Board should also encourage a level of compliance accountability across the organization. A Board may find that not every measure addressed in this document is appropriate for its organization, but every Board is responsible for ensuring that its organization complies with relevant Federal, State, and local laws. The recommendations presented in this document are intended to assist Boards with the performance of those activities that are key to their compliance program oversight responsibilities. Ultimately, compliance efforts are necessary to protect patients and public funds, but the form and manner of such efforts will always be dependent on the organization's individual situation.

Bibliography

Elisabeth Belmont, et al., "Quality in Action: Paradigm for a Hospital Board-Driven Quality Program," 4 Journal of Health & Life Sciences Law. 95, 113 (Feb. 2011).

Larry Gage, *Transformational Governance: Best Practices for Public and Nonprofit Hospitals and Health Systems*, Center for Healthcare Governance (2012).

Tracy E. Miller and Valerie L. Gutmann, "Changing Expectations for Board Oversight of Healthcare Quality: The Emerging Paradigm," 2 Journal of Health & Life Sciences Law (July 2009).

Tracy E. Miller, B*oard Fiduciary Duty to Oversee Quality: New Challenges, Rising Expectations*, 3 NYSBA Health L.J. (Summer/Fall 2012).

Lawrence Prybil, et al., *Governance in Nonprofit Community Health Systems: An Initial Report on CEO Perspectives*, Grant Thornton LLP (Feb. 2008).

Resource 6

The Relationship between the Board of Directors and the Compliance and Ethics Officer

The Relationship between the Board of Directors and the Compliance and Ethics Officer

April 2018

A survey by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association

corporatecompliance.org
hcca-info.org

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Introduction

The relationship between the compliance and ethics officer and the board of directors is both essential and often under developed. When the first version of the survey was fielded in 2010, many compliance professionals were struggling with how to manage what was to many a very new relationship.

Since then a number of factors have changed the dynamic. The Yates memo and increased scrutiny of individual (vs. corporate) actions gained the attention of senior leaders. Later, the Criminal Division of the US Department of Justice issued questions for prosecutors to use as guidance when evaluating compliance programs. Included in them were several about the activities of the board in overseeing the compliance and ethics programs.

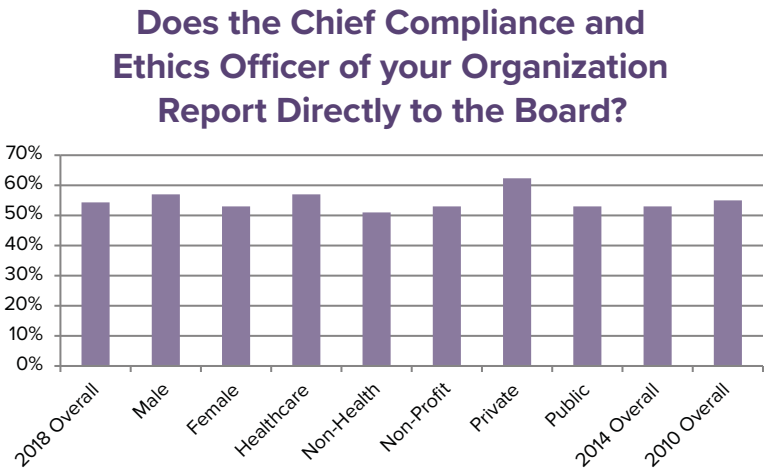
To assess how the relationship between the compliance team and the board had evolved, as well as to examine issues of compliance officer influence, the Society of Corporate Compliance and Ethics and Health Care Compliance Association fielded this survey in 2014 and again in 2018.

Executive Summary

The data reveals that relatively little has changed since the survey results were last released in January 2014. In general, the relationship between boards and the compliance team is seen as a good one. Despite those who argue that compliance should fall under the General Counsel and treat it as the norm, that appears to be the case for only the minority of organizations. Compliance most often reports directly to the board and meets with the board at least four times a year.

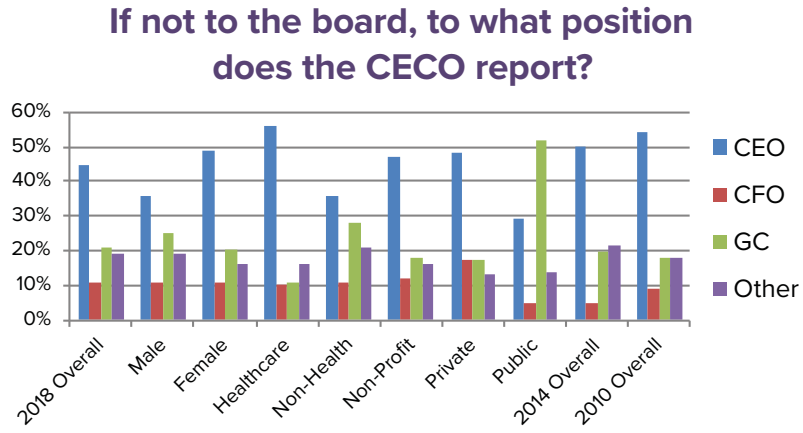
Key Findings

- **Approximately half of compliance officers report to the board.** This is true when looking at the data by industry, ownership (for profit and non-profit) and even by the gender of the compliance officer. Privately held companies were most likely to have a compliance officer reporting to the board (62%). Non-healthcare companies were the least likely (51%) but the difference versus the overall number of 54% was very small.



Society of Corporate Compliance & Ethics / corporatecompliance.org

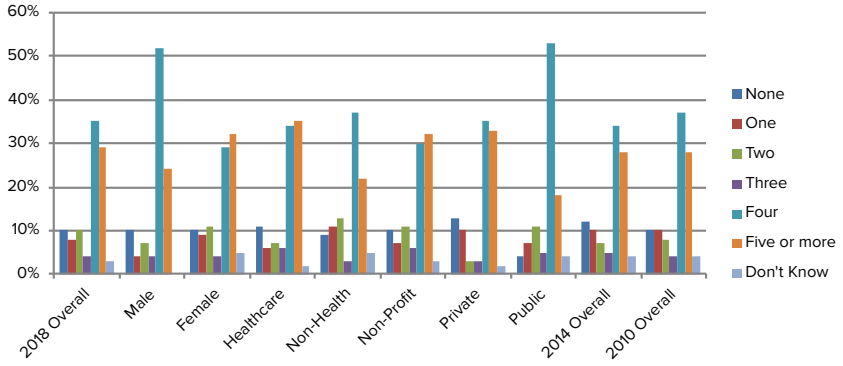
- **Among compliance professionals not reporting to the board, the CEO was the position they were most likely to report to (45%).** There were some notable differences. In healthcare, 56% of those not reporting to the board reported to the CEO. By contrast, for publicly traded companies the figure was just 29%. Women (49%) were more likely to report to the CEO than men (36%). And most notably, only 21% of survey respondents not reporting to the board reported to the GC. Also, potentially of significance, the percentage of respondents who don't report to the board but do report to the CEO has declined over the years from 54% in 2010 to 45% in 2018.



Society of Corporate Compliance & Ethics / corporatecompliance.org

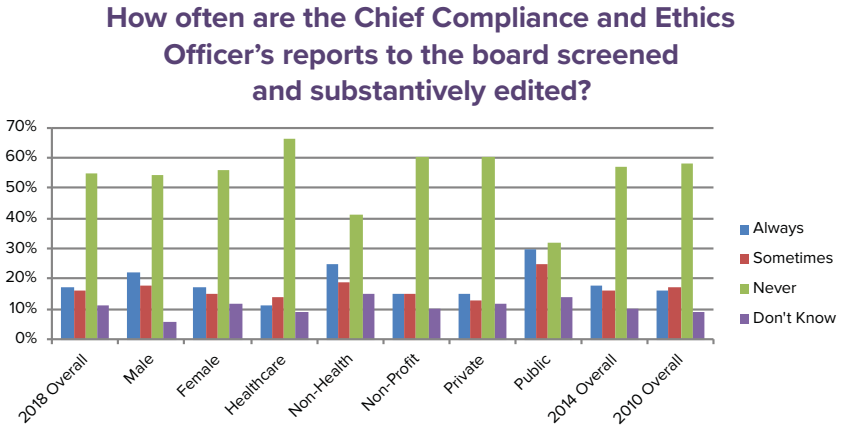
- **Meeting with the board four or more times a year is the norm.** Overall, 35% of respondents reported four regularly scheduled meetings per year, and another 29% reported five or more, bringing the total to 64% with four meetings or more annually.

How many regularly scheduled meetings per year does the Chief Compliance and Ethics Officer have with the board, including board committees?



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **The majority of respondents reported that their reports are not screened by the general counsel or others before being shown to the board.** Healthcare firms particularly stood out in this regard (66% vs. 55%). For publicly traded-firms, though, the likelihood of the report being pre-screened was substantially higher (55% vs 33% of respondents as a whole).



Society of Corporate Compliance & Ethics / corporatecompliance.org

SCCE™
Society of Corporate Compliance and Ethics

TAKE CHARGE OF YOUR COMPLIANCE CAREER

Stay informed on changes affecting the compliance world. Learn from industry experts about emerging best practices for effective compliance and ethics programs.

Join the Society of Corporate Compliance and Ethics

MEMBERSHIP BENEFITS

- *Compliance & Ethics Professional* magazine, 12 issues exclusively for SCCE members plus full access to the magazine archives
- Be a part of a community of 6,500+ Compliance and Ethics Professionals in more than 95 countries
- Member-only discounts on conferences, manuals, and books
- Network locally and globally with 30+ conferences a year at special member rates
- Save on weekly Web conferences for live learning at your desk
- Receive a discount on Compliance Certification Board (CCB)® exam pricing for CCEP and CCEP-I

Additional resources

- Weekly newsletters and blog posts from industry experts
- SCCEnet® provides access to an online Resource Library and networking

LEARN MORE AND JOIN TODAY
corporatecompliance.org/join

- **Generally, compliance officers surveyed were satisfied with the number of meetings with the board each year.** Sixty three percent felt that there were sufficient contacts. Men (78%) tended to be more satisfied with the number than women (59%)

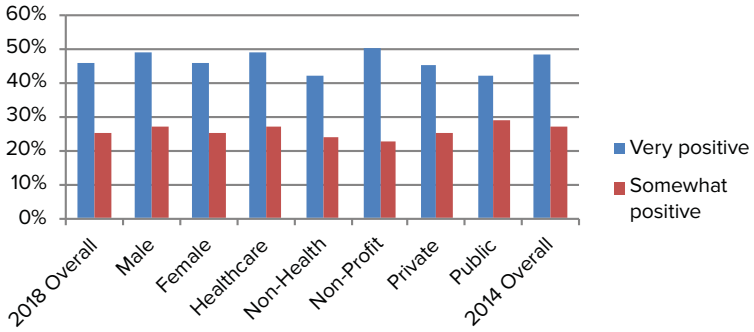
Society of Corporate Compliance & Ethics / corporatecompliance.org

- **One area of possible concern is a declining belief that the board values compliance a great deal.** In 2014, the first year the question was asked, 55% gave the highest mark on this measure. By 2018, the number had declined to 46%. The lowest score (40%) came from survey respondents at privately held companies.

Society of Corporate Compliance & Ethics / corporatecompliance.org

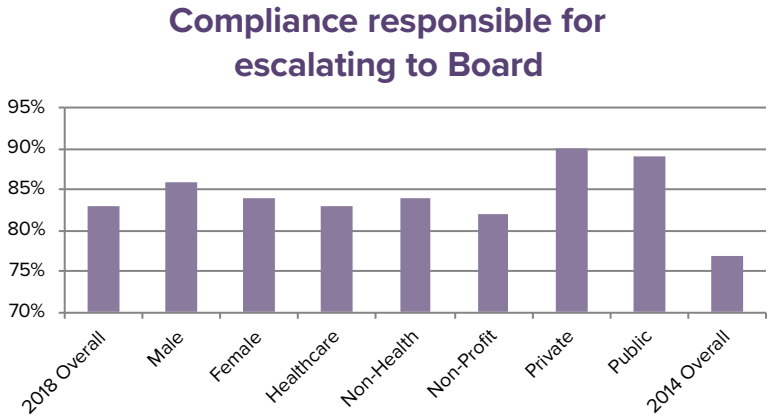
- **In general compliance professionals felt that the quality of the interaction with the board is positive.** The interaction was described as "very positive" by 46% and another 25% rated it as somewhat positive. Only 5% rated it as somewhat or very negative.

How positively would you rate the quality of the interaction of the board with the Chief Compliance and Ethics Officer?



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **Compliance is very much responsible for escalating serious allegations and investigations to the board.** Overall 83% said this was compliance's responsibility either as required by a formal procedure or as a practice.



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **When looking at the attributes for a successful compliance professional, men and women generally had similar opinions.** Survey respondents were given a list of attributes and asked to rate their importance on a 1 to 5 scale, with 5 being most important. While one gender or another might rate an attribute higher on the scale than the other, if looking at the top two highest ratings, they generally were very consistent.

	MEN			WOMEN		
ATTRIBUTES	4	5	4 & 5	4	5	4 & 5
Assertiveness/ Decisiveness	41%	48%	89%	26%	65%	91%
Consensus Building	31%	43%	74%	34%	47%	81%
Confidence	33%	61%	94%	27%	68%	95%
Empathy/Ability to Assess Situation	37%	48%	85%	30%	60%	90%
Independence	22%	69%	91%	17%	77%	94%
Relational/ Interpersonal	31%	53%	84%	22%	68%	90%
Ability to Influence	33%	53%	86%	28%	62%	90%

Conclusions/Implications

- **The role of compliance in organizations seems to be solidified and strong.** The consistency of the data year to year and the overwhelming consistency across the various measures suggests that the position has become an integral one in most organizations with reporting lines to the governing body or very close to it.

- **The idea that compliance reporting to the general counsel is the norm is not born out by the data in the survey or previous ones.** Reporting to the general counsel is the exception, albeit a common one, rather than the rule.

- **Overall the relationship between the board and compliance seems to meet the needs of compliance professionals.** Their general high satisfaction levels with the quality and frequency of the meetings is encouraging.

- **There do appear to be some differences by gender.** Men generally view the relationship more positively and meet with the board more frequently. However, in those cases when compliance does not report to the board, women are much more likely to report to the CEO than elsewhere in the organization

Methodology

Survey responses were solicited and collected during March and April 2018 from compliance and ethics professionals in the database of the Society of Corporate Compliance and Ethics and the Health Care Compliance Association. Additional outreach via social media was also used. Responses were collected and analyzed using SurveyGizmo, a web-based, third-party system. A total of 386 responses were received.

Resource 7

What to Report to Compliance

What to Report to Compliance

- Anti-Kickback
  - Offering items of value to groups who may refer patients to the hospital
    - Gift basket to private physician office
  - Giving or receiving free items or discounts
    - Vendor offering sports tickets in return for purchasing product
- Claims/Billing Process
  - Duplicate billing
  - Billing for services not medically necessary
  - Inaccurate coding or billing
- Conflict of Interest
  - Any situation where job performance or decision making is influenced by anything other than patient needs or hospital interests
- Copyright
  - Copying of print or electronic books, journals, or other publications
- Documentation
  - Incomplete documentation
    - Missing consents or notes
  - Inaccurate documentation
- Human Resources
  - Discrimination
  - Labor law violations
- Identity Theft
  - Patient registering under false name
- Inducement
  - Offering items of value to influence a Medicare/Medicaid beneficiary to choose the hospital
    - Routine waivers of co-pays and deductibles
- Medical Staff/Stark
  - Provider financial/compensation arrangements
  - Non-monetary compensation
    - Dinners or gifts for physicians provided by the hospital
- Privacy/Security
  - HIPAA violations/breaches – even incidental – any wrongful access/disclosure
  - Fax sent to incorrect number
  - Paperwork given to wrong patient
  - Test results sent to incorrect physician
  - Social media posts regarding patients or patient care