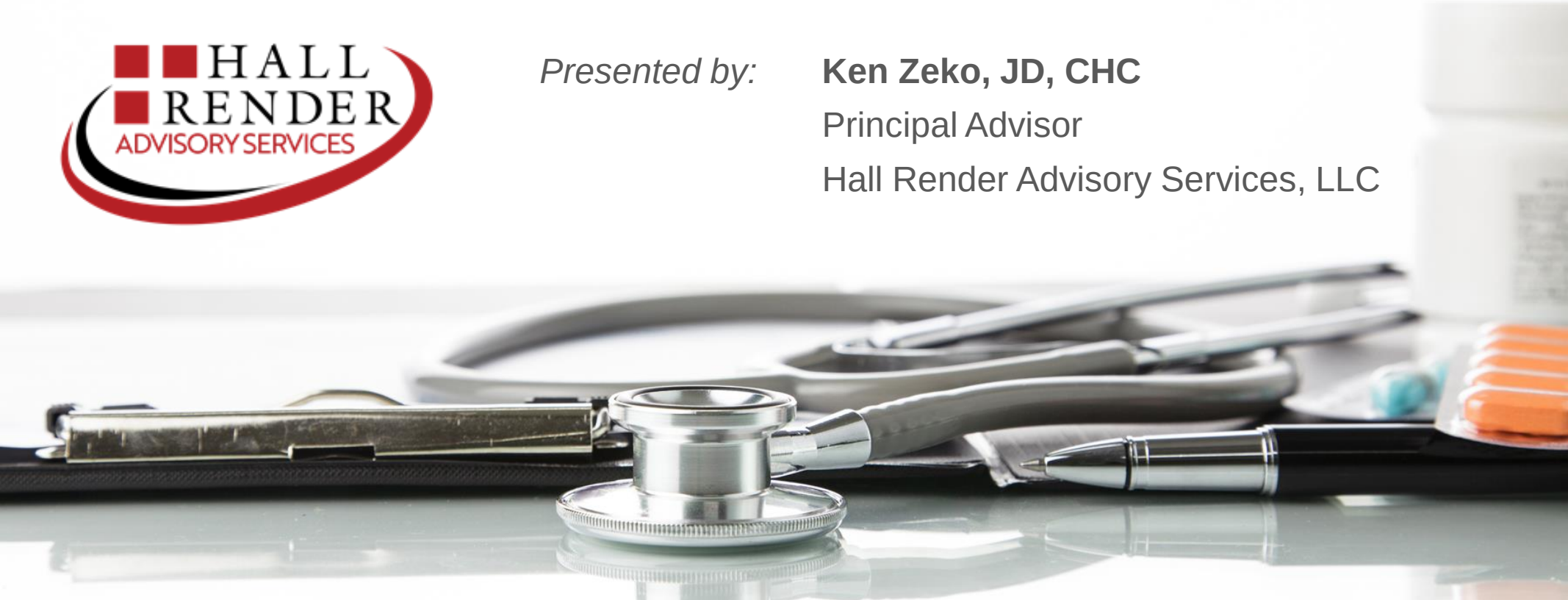
The Importance of Effective Compliance Programs

Presented by: **Ken Zeko, JD, CHC**
Principal Advisor
Hall Render Advisory Services, LLC



Overview

- What should a Compliance Program look like?
- Understanding and embedding the Three Lines Risk Model into operations
- Government data analytics capabilities
- Promoting organizational cultures that encourage ethical conduct and are conducive to employees doing compliance activities

What Should a Compliance Program Look Like?

Origins of Compliance Programs

Compliance Guidance

OIG has developed a series of voluntary compliance program guidance documents directed at various segments of the health care industry, such as hospitals, nursing homes, third-party billers, and durable medical equipment suppliers, to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements.

See: https://oig.hhs.gov/compliance/compliance-guidance/

What Should a Compliance Program Look Like?

Effective compliance programs should mitigate/eliminate regulatory/criminal risks, **promote an organizational culture that encourages ethical conduct** and provide organizations with the ability to defend against allegations of fraud or abuse.

Incorporated into the OIG's various Compliance Program Guidance Documents and promulgated in the Federal Sentencing Guidelines; the Seven Elements represent the basic tenets of an effective compliance program.

Oversight
Compliance Office & Committee
Oversight Boards

Written Standards
Code of Conduct
Policies & Procedures
Event/Function specific guidance documents

See: https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/GLMFull.pdf and https://oig.hhs.gov/compliance/compliance-guidance/

What Should a Compliance Program Look Like?

Training
Adequate training on company specific compliance polices and expectations.
Should include all relevant employees and 3rd party agents working on behalf of the organization.

Disciplinary Guidelines and Enforcement of Company Standards
Clear, specific and transparent disciplinary policies
Consistency with consequences
Intentional/material vs. negligent violations

Communication
Anonymous Compliance Hotline
Access to supervisors and compliance personnel
Positive compliance tone from leadership

Responding to Detected Problems & Corrective Action
Investigations process/Root Cause
Development and corrective action/mitigation plan

Risk Based Auditing & Monitoring
Risk Assessment
Internal and 3rd party auditors
Business-based monitoring

Understanding and Embedding the Three Lines Risk Model into Operations

Three Lines Model

"The Third Line"

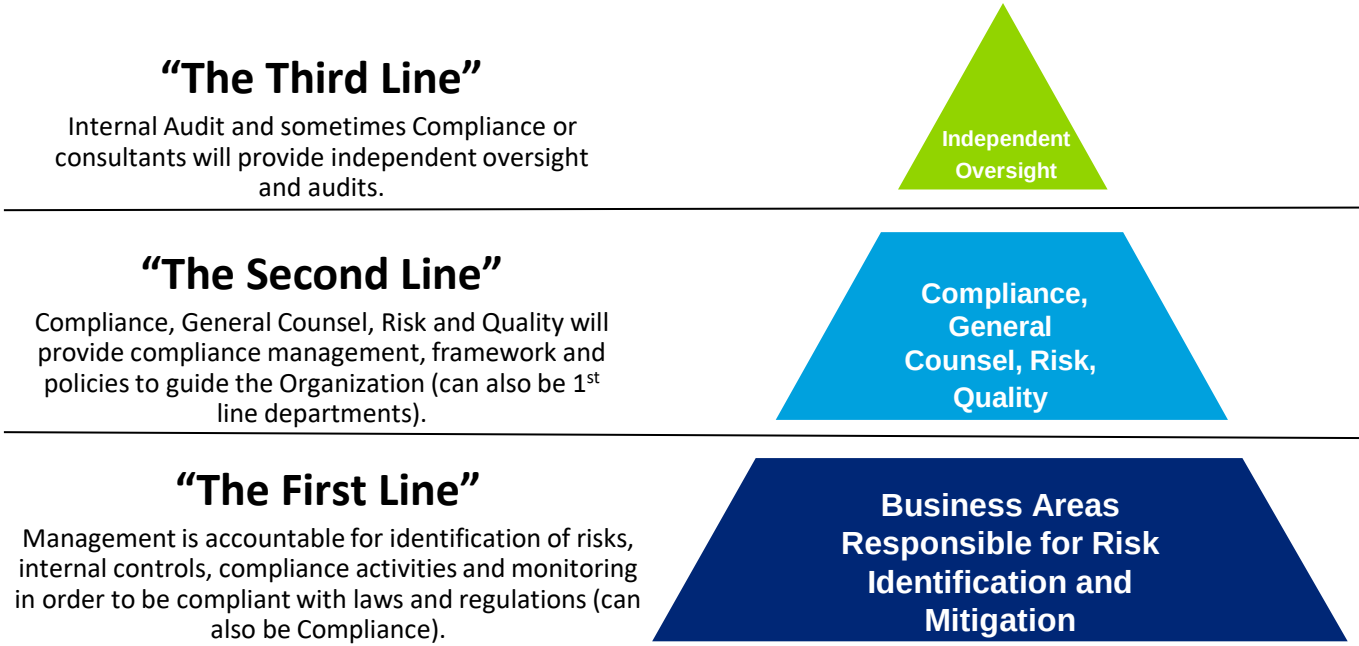
Internal Audit and sometimes Compliance or consultants will provide independent oversight and audits.

"The Second Line"

Compliance, General Counsel, Risk and Quality will provide compliance management, framework and policies to guide the Organization (can also be 1st line departments).

"The First Line"

Management is accountable for identification of risks, internal controls, compliance activities and monitoring in order to be compliant with laws and regulations (can also be Compliance).



See: https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf

Auditing vs. Monitoring

"Auditing: Auditing is a formal, systematic and disciplined approach designed to evaluate and improve the effectiveness of processes and related controls. Auditing is governed by professional standards, completed by individuals independent of the process being audited, and normally performed by individuals with one of several acknowledged certifications. Objectivity in governance reporting is the benefit of independence.

Typical characteristics of an audit include the following:

- Formal review governed by professional standards
- Completed by professionals independent of the operation
- Formal, systematic and structured approach
- Involves planning, sampling, testing, and validating
- Formal communication with recommendations and corrective action measures
- Documented follow-up of corrective actions
- Audit accountability is typically to the Chief Audit Executive and the Audit Committee
- Involves routine, formal communication to the Board and Management"

See: https://ahia.org/assets/Uploads/pdfUpload/WhitePapers/DefiningAuditingAndMonitoring.pdf

Ex: Physician Arrangements Auditing

The following are some possible physician arrangements audits that can be completed to test whether policies and procedures exist, including the following elements and controls:

- Requirements for the initiation, review, approval and monitoring of physician contracts;
- A process for including the roles of General Counsel and Finance, use of templates, documentation of Fair Market Value (“FMV”) and a process for approving compensation that is substantially higher than FMV;
- Process for managing contracts after they are executed;
- Process for reviewing and approving payments to ensure payments are being made in accordance with the terms of the agreement;
- Process for monitoring that the services required by the contract are being performed, including the requirement for the physician to provide a time log for all administrative services contracts, and
- Requirements for monitoring physician leases and invoicing tenants for late fees when required by the leases.

Auditing vs. Monitoring

"Monitoring: Monitoring is an on-going process usually directed by management to ensure processes are working as intended. Monitoring is an effective detective control within a process.

Typical characteristics of monitoring efforts include the following:

- Often less structured than auditing, though audit techniques may be employed
- Usually completed by operations or compliance personnel
- Involves on-going checking and measuring
- Can be periodic spot checks, daily/weekly/monthly tests
- May identify the need for an audit
- Accountability for monitoring is typically to operations leadership
- Typically completed by department staff and communicated to department management
- If completed in relation to a compliance work plan, formal communication to Chief Compliance Officer and Compliance Committee
- May involve internal audit or compliance"

See: https://ahia.org/assets/Uploads/pdfUpload/WhitePapers/DefiningAuditingAndMonitoring.pdf

Ex: Coding/Billing Monitoring

Monitoring activities can and should be completed throughout the organization and assigned with consideration of the person's role and responsibilities.

Operational leadership should be able to report to the Compliance Committee the specific steps and processes implemented to monitor coding compliance and mitigate False Claims risk and the frequency these activities are performed. The following are examples of coding/billing monitoring activities according to individual's roles:

- **Credentialing Manager**: monitors complete and timely credentialing of onboarded providers
- **Department Manager**: runs daily, weekly, quarterly reports to identify outliers
- **Office Manager**: checks certifications & recertifications are present and signed
- **Billing and Coding Manager**: monitors coding anomalies, modifier application, schedules and delegates baseline audits prospectively and follow-up, provider schedules for Incident-to services
- **Billing and Coding Staff**: monitors for complete records, appendage of signatures, and completes internal audits as assigned by Billing and Coding Manager

Lack of a True Operational Compliance Committee

Depending on the size of some organizations, the Operational Compliance Committee would likely consist of approximately 10 – 20 people. Participants are optimally not part of the executive team but are department leaders or their delegates. Typical committee representation may include the following functions:

- Chief Compliance Officer – Chair
- Legal/Risk
- HIM
- Utilization Management
- Quality
- Revenue Cycle/Finance
- Pharmacy
- Laboratory
- Research
- Admitting/Registration
- Emergency Department
- Radiology
- Physician Leadership
- Nursing
- Information Systems
- Human Resources
- Health Plan
- HIPAA Privacy and Security
- Provider Services

Lack of a True Operational Compliance Committee

The typical functions of the Operational Compliance Committee are:

- Assist and advise Compliance Officer with all aspects of the compliance program
- Develop, implement and report on compliance efforts occurring in their respective department
- Assist in monitoring the effectiveness of the overall Compliance program
- Assist with compliance risk identification and risk mitigation
- Assess and advise on compliance policies and procedures
- Oversee and advise on Compliance training
- Oversee compliance auditing and monitoring
- Assess and advise on reported compliance matters
- Oversee the status of corrective actions
- CONDUIT TO ACCOUNTABILITY

Lack of a True Operational Compliance Committee

The meetings are expressly and solely dedicated to Compliance issues and the Committee establishes accountability for ongoing Compliance risk monitoring to the operational leaders on the committee.

A typical agenda would include the discussion of:

- Regulatory and Compliance updates
- Operational Compliance monitoring and auditing activities by each member of the committee
- Compliance training
- Actions to continue to enhance each of the 7 elements of an effective Compliance program
- Addressing ad-hoc compliance issues

It is common for such committees to invite guests that may offer a topically relevant view-point as appropriate.

Government Data Analytics Capabilities

Data Analytics

Commercial Payors and the Government's use of Data Analytics have:

- Changed the way they do their jobs
- Increased productivity
- Increased collaboration
- Improved ability to detect fraud, waste and abuse

Health Care Fraud and Abuse Control Program (HCFAC)

"The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a national **Health Care Fraud and Abuse Control Program** (HCFAC or the Program) under the joint direction of the Attorney General and the Secretary of the Department of Health and Human Services (HHS), acting through the Inspector General, designed to coordinate federal, state, and local law enforcement activities with respect to health care fraud and abuse."

"The return on investment (ROI) for the HCFAC program over the last three years (2020–2022) is $2.90 returned for every $1.00 expended. The ROI has been adversely impacted by the COVID19 pandemic."
https://oig.hhs.gov/publications/docs/hcfac/FY2022-hcfac.pdf

OIG Data Analytics

" HCFAC funding supports HHS-OIG's advanced data analytics initiatives to expand our tools, models, and customized analytics with artificial intelligence (AI) and cloud computing to: (1) proactively monitor and target our oversight of high-risk HHS programs and health care providers; (2) identify trends, outliers, and potential investigative or audit targets; (3) enhance decision making; (4) optimize HHS-OIG processes; and (5) support mission needs.

"HHS-OIG applies predictive and geospatial analytics, leverages dashboards, machine learning, and AI capabilities including neural networks and text mining to identify and support prosecutions…

More than 760 unique staff members used HHS-OIG analytic tools for mission-focused work to generate more than 44,000 provider-specific reports and claims exports, page views, and other analytic insights, during the fiscal year.."

https://oig.hhs.gov/publications/docs/hcfac/FY2022-hcfac.pdf

The Fraud Prevention System (FPS)

"FPS is the predictive analytics technology required under the Small Business Jobs Act of 2010. FPS analyzes FFS claims using sophisticated algorithms to target investigative resources; generate alerts for suspect claims or providers and suppliers; and provide information to facilitate and support investigations of the most egregious, suspect, or aberrant activity."

"During FY 2022, the FPS generated alerts that resulted in 960 new leads for program integrity contractors and augmented information for 759 existing leads or investigations. The program integrity contractors reported initiating FPS-attributable actions against 786 providers in FY 2022."

https://oig.hhs.gov/publications/docs/hcfac/FY2022-hcfac.pdf

Integrated Data Repository and the One Program Integrity (One PI) Portal

"One PI provides CMS program integrity contractors, law enforcement personnel, HHS-OIG investigators, and other organizations a centralized single access point to analytical tools and data needed to fight Medicare and Medicaid fraud, waste, and abuse. One PI provides access to Medicare and Medicaid data from the Integrated Data Repository (IDR), which allows users to investigate improper payments, identify fraud schemes, create and enhance fraud prevention models, take administrative actions, pursue civil and criminal penalties, and more to protect Medicare and Medicaid taxpayer dollars."

"CMS is currently working to integrate One PI with the Unified Case Management (UCM) system and the FPS to become the centralized reporting hub for CMS."

https://oig.hhs.gov/publications/docs/hcfac/FY2022-hcfac.pdf

Healthcare Fraud Prevention Partnership

"Public and private sector organizations have long recognized the need for coordination, data, and information-sharing to combat health care fraud. In 2012, the HFPP was formed as a public-private partnership consisting of 21 Partners. Since its inception, the importance and value of the HFPP's mission has driven significant growth in its membership.

Today, the HFPP has a broad membership comprised of 304 Partners, making it uniquely positioned to examine emerging trends and develop key recommendations and strategies to address them.

The HFPP first began with professional claim types only, then expanded in 2019 to include institutional claims. In 2021, pharmacy claims were added for more comprehensive analytic insights.

Starting initially with original claims data, the Partnership is now conducting its analysis against adjusted claims to detect industry-wide fraud schemes more precisely."

https://www.cms.gov/hfpp/about

Healthcare Fraud Prevention Partnership

"The HFPP's primary goal is to help Partners move from a reactive approach to a preventative approach to identify and address fraud by generating comprehensive strategies that each Partner can use to combat healthcare fraud, waste, and abuse.

- Unparalleled Data Source: The HFPP represents the full spectrum of healthcare payers and anti-fraud associations, which enables data, information sharing, and sophisticated data analytics against a unique cross-payer data set.

- Collaboration & Strategic Partnerships: Through a variety of HFPP events, Partners leverage their collective experiences to meaningfully participate and guide the Partnership."

https://www.cms.gov/hfpp/about

Healthcare Fraud Prevention Partnership

Consolidated Appropriations Act – Signed into Law December 27, 2021

Codified the public-private partnership to detect fraud, waste and abuse in health plans. HHS shall enter into a contract with a trusted third party for purposes of carrying out the duties of the partnership.

42 USC 1320a-7c: Fraud and abuse control program

The partnership shall-

(i) provide technical and operational support to facilitate data sharing between partners in the partnership;

(ii) analyze data so shared to identify fraudulent and aberrant billing patterns;

(iii) conduct aggregate analyses of health care data so shared across Federal, State, and private health plans for purposes of detecting fraud, waste, and abuse schemes;

(iv) identify outlier trends and potential vulnerabilities of partners in the partnership with respect to such schemes;

(v) refer specific cases of potential unlawful conduct to appropriate governmental entities;

(vi) convene, not less than annually, meetings with partners in the partnership for purposes of providing updates on the partnership's work and facilitating information sharing between the partners;

(vii) enter into data sharing and data use agreements with partners in the partnership in such a manner so as to ensure the partnership has access to data necessary to identify waste, fraud, and abuse while maintaining the confidentiality and integrity of such data;

(viii) provide partners in the partnership with plan-specific, confidential feedback on any aberrant billing patterns or potential fraud identified by the partnership with respect to such partner;

(ix) establish a process by which entities described in subparagraph (A) may enter the partnership and requirements such entities must meet to enter the partnership;

(x) provide appropriate training, outreach, and education to partners based on the results of data analyses described in clauses (ii) and (iii); and

(xi) perform such other duties as the Secretary determines appropriate

Healthcare Fraud Prevention Partnership

As of September 10, 2023, the HFPP had a total of 304 Partners:

- 6 Federal Partners
- 81 Law Enforcement Partners
- 139 Private Payor Partners
- 50 State Medicaid Partners
- 15 Associations
- 13 Other State and Local Partners

https://www.cms.gov/files/document/hfpp-fact-sheet.pdf

Data Analytics – Governmental Audits

The Government has an alphabet soup of governmental agencies performing data analytics and audits to reduce fraud and waste:

- HEAT: Healthcare Fraud Prevention & Enforcement Action Team
- MIC: Medicaid Integrity Contractor
- Medicaid RAC: Medicaid Recovery Audit Contractor
- RAC: Medicare Recovery Contractor
- ZPIC: Zone Program Integrity Contractors
- UPIC: Unified Program Integrity Contractors
- MAC: Medicare Administrative Contractor

Data Analytics – Governmental Audits

"The MACs and UPICs shall have available sufficient hardware, software, and personnel with analytical skills to meet requirements for identifying problems efficiently, and effectively developing and implementing corrective actions. If MACs are unable to employ staff with the qualifications necessary for effective data analysis, evaluation and reporting, they shall use other entities (e.g., universities, consultants, other contractors) who can provide the technical expertise needed."

https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/pim83c02.pdf

Data Analytics – Payor Audits

Commercial Payors, Medicare Advantage, Medicaid Managed Care Organizations (MCO), CHIP MCOs all have Special Investigative Units (“SIU”)

What is an S.I.U?

- The Special Investigation Unit, is a department within an insurance company with a targeted focus on recovering payments from medical providers that appear to be the product of fraud, waste or abuse.
- These units utilize data analytics to focus on providers that fall out of the normal range.
- SIUs are incentivized to discover and recover inappropriate payments to providers.

The Yates Memo (2015)

1. In order to qualify for any cooperation credit, corporations must provide to the Department of Justice (DOJ) 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 DOJ will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation.
5. DOJ 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.
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 Yates Memo and DOJ Updates

- In speeches on October 28, 2021, and September 15, 2022, Deputy Attorney General Lisa O. Monaco issued additional guidance regarding the Yates Memo and holding individuals accountable.
- Monaco stated,
  - "To hold individuals accountable, prosecutors first need to know the cast of characters involved in any misconduct. To that end, today I am directing the department to restore prior guidance making clear that to be eligible for any cooperation credit, companies must provide the department with all non-privileged information about individuals involved in or responsible for the misconduct at issue. To be clear, a company must identify all individuals involved in the misconduct, regardless of their position, status or seniority."
  - "Let me start with our top priority for corporate criminal enforcement: going after individuals who commit and profit from corporate crime."

See: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute and https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement

Lessons Learned

Tone at the Top per U.S. DOJ Evaluations of Corporate Compliance Programs

"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 clearly 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."

"How have senior leaders, through their words and actions, encouraged or discouraged compliance…?"

"What concrete actions have they taken to demonstrate leadership in the company's compliance… efforts? How have they modelled proper 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?"

"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…? Have they persisted in that commitment in the face of competing interests or business objectives?"

Promoting Organizational Cultures that Encourage Ethical Conduct

Tools for Compliance Programs

- Chapter 8 of the Federal Sentencing Guidelines states, “organizations shall… promote an organizational culture that encourages ethical conduct.”
- Consider requiring employees and exiting employees to complete Integrity or Culture Surveys.
- Analyze and track and trend exit surveys and turnover.
- Investigate perceptions/allegations of toxic employees.
- Analyze hotline calls to determine if a high percentage of calls are about certain employees who may be negatively impacting the organization’s culture.
- Assess stories/perceptions from exiting employees, hotline calls, and turnover to identify to what extent there are risks that impact organizational culture.

https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8

"What we've got here is a failure to communicate." See: Cool Hand Luke

- After conducting countless interviews with CEOs, it's apparent that most CEOs assume employees understand what the organization's culture is.

- Often CEOs and the Leadership team are too busy to realize the need to describe the desired organizational culture, and they're unaware that a large number of employees can't describe the organization's culture, and therefore, can't aspire to reach the desired organizational culture.

- Leadership retreats are often devoid of conversations regarding what the organization's culture is and how it is to be attained.

Questions to Ask

- Has the organization and specifically the CEO overtly described the desired organizational culture?
- Can employees describe the organization's culture?
- Has the Compliance Department provided the CEO and Leadership team with venues/opportunities to overtly describe the organization's culture?
- Does the organization, CEO, and Leadership team use stories and examples when describing the organizational culture?
- Are employees formally rewarded/recognized for exhibiting the desired organizational culture?
- Are efforts to raise awareness, such as including a description of the organization's desired culture in training activities, town halls, huddles, and newsletters, tracked and trended and reported to the Operational Compliance Committee?

HALL RENDER
ADVISORY SERVICES

Should you have any questions or comments or require additional information, please contact us.

Ken Zeko, JD, CHC
214-458-3457
kzeko@hallrenderAS.com