BRG

Qui Tam & Civil False Claims and Healthcare Fraud Institute 2026

Compliance Programs, Corporate Integrity Agreements, Independent Review Organizations, and Board Experts

ABA AMERICANBARASSOCIATION

Panelist Introductions

Wendy Millette
Panelist

WENDY MILLETTE is an Executive Vice President and the Global Chief Compliance Officer for Fresenius Medical Care, a global provider of products and services for people with chronic kidney failure. Wendy is responsible for implementing and maintaining an effective compliance program while supporting her businesses to grow and innovate. She oversees a team of compliance professionals in 50 countries. Wendy has held various legal, regulatory, and compliance leadership positions over her 18-year tenure at Fresenius Medical Care. Wendy started her career as a litigation attorney at Holland & Knight LLP in Boston.

Meredith Williams
Panelist

MEREDITH WILLIAMS is Counsel at Barnes & Thornburg, where she advises healthcare and life sciences clients on federal fraud and abuse compliance, regulatory strategy, and government investigations. She brings more than 20 years of experience from the U.S. Department of Health and Human Services Office of Inspector General (OIG), where she served in senior legal roles spanning enforcement, advisory opinions, and regulatory guidance. Meredith has deep expertise in the Anti-Kickback Statute, Civil Monetary Penalties law, and False Claims Act enforcement, and regularly assists clients with compliance program design, investigations, and interactions with government regulators.

Steve Ortquist
Panelist

STEVE ORTQUIST is Founder and Managing Director of Arete Compliance Solutions, where he advises healthcare organizations on the design, implementation, and effectiveness of compliance programs. He has served as Chief Compliance Officer and senior compliance executive at major health systems, including Banner Health, Tenet Healthcare, and Sutter Health, and has extensive experience managing Corporate Integrity Agreements and government investigations. Steve is a recognized leader in healthcare compliance, with deep expertise in risk assessment, program development, and remediation, and is a frequent speaker and advisor on compliance and enforcement matters. [aretecompliance.com]

Tom O'Neil
Moderator

TOM O'NEIL is a Managing Director at BRG, where he leads the firm's Healthcare Governance, Compliance, and Ethics advisory practice. He is a highly respected advisor and corporate director with broad private and public sector experience, including leadership roles in the boardrooms and C-suites of companies in the healthcare industry sector. He currently serves on four corporate boards of directors, including as the Chair of a mutual fund board. He also serves as the Chair of the Ethics, Compliance and Quality Committees of two privately held healthcare company boards, one operating in the home health and hospice segment and the other an independent provider of integrated pharmacy solutions. He was recently appointed to the Board of Directors of a private paratransit company and serves as the Chair of the Board's Audit and Risk Oversight Committee.

Table of Contents

BRG

Compliance and Ethics Program Design and Operational Effectiveness

The Foundational "Seven Elements"

- In the 1980s, OIG released its first iteration of compliance and ethics program guidance. It focused on certain critical controls and functions that are often cited as the "Seven Elements of an Effective Healthcare Compliance Program."
- Agency guidance has since evolved, focusing on operational efficacy.

Element or Function	Initial Guidance (OIG Compliance Program Guidance, 1998-2008)
Designation of Chief Compliance Officer and Compliance Committee	The Company has a functioning Compliance Officer and Compliance Department. The Compliance Officer reports to the Chief Executive Officer (CEO) and Board of Directors. A Compliance Committee, composed of senior company officers, meets on a regular basis to oversee the Company's Compliance efforts.
Compliance Policies and Procedures Including Standards of Conduct	The Company adopts a Code of Conduct and the Compliance Department reviews and revises all compliance policies and procedures and related corporate policies covering compliance with laws and regulations.
"Open Lines of Communication"	The Compliance Officer reports to the Board of Directors. The Company maintains both a 24 hour / 7 day a week Compliance and Ethics Action line, a compliance "e-mail" box and other mechanisms for bringing forth compliance issues.
Training and Education	Company has mandatory, annual compliance and ethics training for all employees. Additional and special compliance training is conducted for coding & billing employees, particularly around issues of Medicare/Medicaid regulations and medical necessity.
Response to Detected Offenses	Company investigates and responds to all compliance issues and complaints. Compliance maintains an electronic tracking system for compliance issues.
Internal Monitoring and Auditing	The Compliance Department, in concert with the senior officers on the Compliance Committee, conducts an annual compliance "risk assessment" process to design and conduct the annual auditing and monitoring plan.
Enforcement and Disciplinary Standards	Code of Conduct provides that the Company will take disciplinary action – including termination – against employees who violate compliance policies or procedures. Appropriate disciplinary actions have been documented in the issues log.

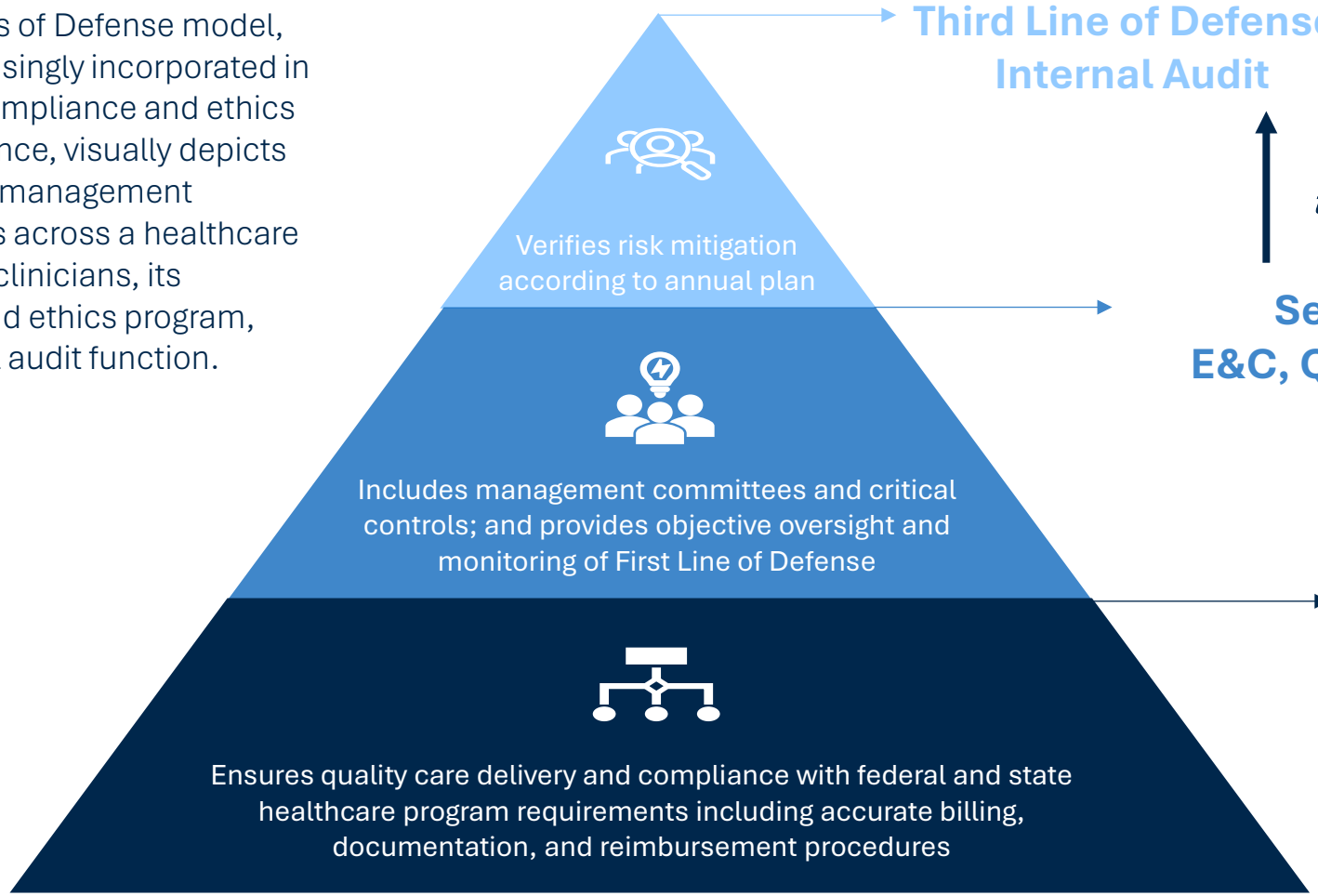
Stakeholder Expectations: The Next Chapter

- Many well-meaning organizations implemented agency guidance as a checklist, creating "paper" or "shelf" compliance programs that emphasized formal existence over functional effectiveness. **Over time, it became clear that merely establishing core controls and meeting threshold requirements was insufficient to ensure an effective compliance program.**
- In practice, **many programs proved to be operationally ineffective due to inadequate resourcing** that was not meaningfully embedded across the organization, **a lack of shared ownership** beyond the compliance function, **and implementations that were primarily defensive** rather than designed to proactively manage and mitigate risk.
- Understandably, this led stakeholders to expand the focus to include:

Organizational Values and Culture
Governance and Oversight
Periodic, Comprehensive Risk Assessments
Development and Execution of Annual Work Plans
Root Cause Analyses and Corrective Action Plans
Quality Control of Ongoing Auditing, Testing, and Monitoring
Periodic Independent Program Assessments

The Three Lines of Defense Model for Enterprise Risk Management

The Three Lines of Defense model, which is increasingly incorporated in stakeholder compliance and ethics program guidance, visually depicts enterprise risk management responsibilities across a healthcare organization's clinicians, its compliance and ethics program, and its internal audit function.



Third Line of Defense: Internal Audit

The Second Line's findings inform the Third Line's priorities.

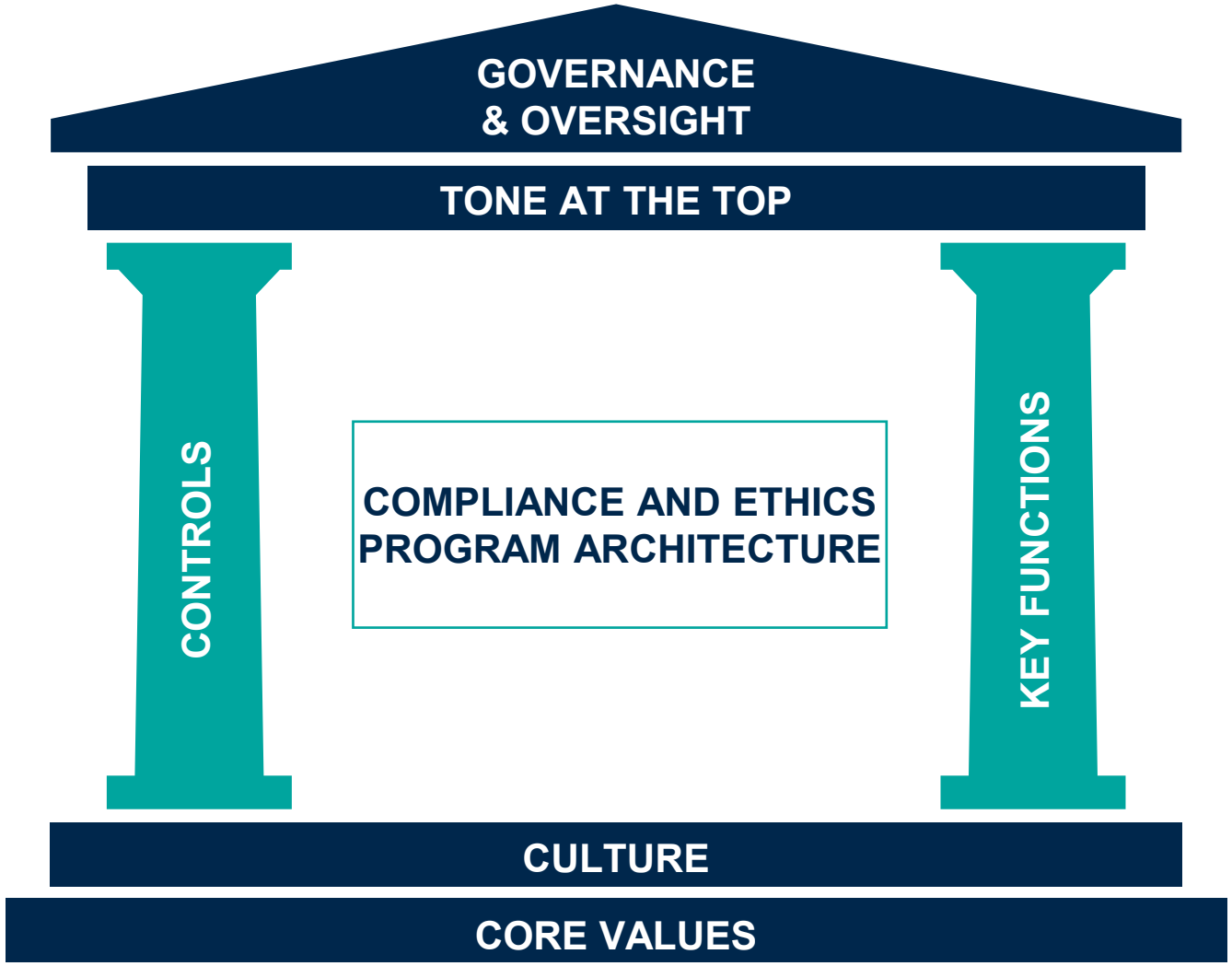
Second Line of Defense: E&C, Quality and Enterprise Risk Programs

The First and Second Lines must collaborate effectively.

First Line of Defense: Front-line Operational Controls

Program Architecture

- This graphic illustrates the architecture of an effective compliance and ethics department:
  - Culture and core values serve as the foundation;
  - Controls and key functions hold the program together; and
  - Leaders ensure appropriate oversight and Tone at the Top to reinforce the program.



Hallmarks of Effective Compliance and Ethics Programs

Successful compliance and ethics programs are driven by neither fiat nor fear, but by **powerful core values** and a cohesive organizational culture led by an **ethical North Star**.

- They require a high level of leadership engagement, with clear accountability, operational transparency, and a credible "Open Door" environment.
- Employees must understand and embrace institutional commitments to integrity and acceptance of responsibility.
- Quite apart from regulatory and enforcement agency expectations, a best-in-class enterprise compliance and ethics program can be a market differentiator.

- **There is no "one-size-fits-all" formula for an effective program.** The design and implementation must be informed by the size of the company, the industries and geographic markets in which it operates, its business activities, and the organization's risk appetite.
- Effective compliance and ethics programs:
  - Are driven by compelling **core values** and **unequivocal sponsorship** by the senior leadership team;
  - Are **overseen by a board of directors** or governing body;
  - Have a **strong ethical dimension** and enable strategic success through risk-informed collaboration;
  - Include effective and **robust reporting channels** – "up and out";
  - Identify, assess, prioritize, and remediate risks through a **cohesive and scalable framework** that includes an enterprise lens;
  - Include **systemic verification initiatives** such as audits, testing, and monitoring;
  - Ensure that business units, and product and service lines, have the **requisite expertise, support and resources**; and
  - Are committed to **operational transparency, continued self-improvement and periodic self-assessment**.

Living Under a Corporate Integrity Agreement (CIA)

Overview

- Violations of federal healthcare laws and regulations can result in civil actions, criminal prosecutions, the payment of substantial penalties, and most notably, **exclusion from participating in federal healthcare programs.**
- OIG has both mandatory and permissive exclusion authority. When exercising its permissive authority, OIG often requires organizations to enter into a CIA to avoid exclusion.
- **A CIA is a detailed operational agreement that typically lasts 5 years and is tailored to address the problematic conduct that OIG identified during its investigation.** CIAs also offer valuable insight into OIG's evolving expectations for effective governance, as well as quality and safety and compliance and ethics programs. They generally establish comprehensive obligations regarding:

Compliance and Ethics Program Design and Operational Effectiveness	Periodic Reports and Certifications by the Organization
Amplified Transparency	Independent Reviews and Assessments to Verify Compliance with CIA Obligations

- CIAs are designed to **remediate identified misconduct, impose structural and operational controls, and provide direct OIG visibility into compliance performance.**
- Unlike baseline compliance program expectations, a CIA is prescriptive (not principles-based), externally monitored, and contractually enforceable.

Core CIA Obligations

CIAs translate enforcement findings into codified, operational requirements:

Governance and Oversight	• Board-level compliance obligations and certifications; and • Designation and authority of Chief Ethics and Compliance Officer.
Policies, Procedures, and Training	• Targeted policies tied to risk areas; and • Annual training and certifications.
Auditing and Monitoring	• Risk-based internal audits; and • Independent Review Organization (IRO) testing.
Reporting and Disclosure	• Mandatory disclosure of reportable events; and • Annual reports to OIG.
Corrective Action	• Formalized remediation and discipline processes; and • Root cause analysis expectations.

Reporting, Certification, and OIG Oversight

- OIG oversight of a CIA is continuous, rigorous, and grounded in mandatory reporting obligations.
- Organizations subject to a CIA are required to submit **implementation and annual reports to OIG detailing the design, operation, and effectiveness of their compliance program**, including audit results, identified risk areas, and corrective actions taken.
- These reporting obligations are paired with **affirmative certifications by executive leadership and, increasingly, the board**, reflecting OIG's expectation that senior leadership is not only informed, but actively accountable for compliance performance and program effectiveness.
- CIAs also impose **mandatory disclosure obligations for specified "Reportable Events," which typically must be reported within defined timeframes and include probable violations of federal healthcare program requirements, significant overpayments, the employment of ineligible persons, and ongoing investigations or legal proceedings.**
- In addition, IRO findings are submitted directly to OIG as part of the reporting framework, providing an external, technical validation of compliance in defined risk areas such as claims accuracy and regulatory compliance.

Operational Realities of Implementing a CIA

- Operating under a CIA **fundamentally reshapes how an organization functions on a day-to-day basis.**
    - **Governance becomes structured and highly formalized.** Board and committee activities become more frequent, more documented, and more closely tied to compliance and ethics performance, with escalation pathways and oversight mechanisms subject to scrutiny.
    - **Compliance becomes operationalized across the enterprise.** Business units must translate CIA requirements into daily processes, controls, and decision-making frameworks, rather than relying solely on the compliance and ethics function.
    - **Documentation serves as a core control.** Organizations must demonstrate that compliance activities are not only performed, but contemporaneously documented, auditable, and capable of external review.
    - **Issue management takes on heightened significance.** Potential compliance and ethics concerns are evaluated through a "Reportable Event" lens, requiring rapid escalation, investigation, and resolution under defined timelines.
    - **Resource demands increase materially.** Organizations must dedicate significant personnel, financial, and technological resources to support auditing, monitoring, reporting, and external validation requirements.
- In practice, a CIA creates a parallel operating environment characterized by continuous OIG oversight and organized accountability.

The Role of an IRO in CIA Oversight

Overview

- An IRO is a third-party engaged under a CIA **to provide objective, programmatic validation of compliance in defined risk areas.**
- IROs are required in most CIAs as an integral component of OIG's oversight framework. They typically focus on claims and coding compliance, quality and safety, and financial relationships and arrangements.
- **IROs operate as an external assurance function that is distinct from internal audit, compliance, and legal.**
- The role of IROs is best understood as part of a three-stage model:

Stage	Function	Owner
Design	Policies, controls, program architecture	Compliance
Implementation	Operational execution and controls	Business
Validation	Independent programmatic testing	IRO (External)

- IROs help ensure OIG **that compliance is not only designed and implemented, but independently verified through objective testing.**

Scope and Methodology of IRO Reviews

- IRO reviews are defined by the CIA and are designed to produce **objective, statistically valid, and repeatable assessments of compliance in specified risk areas.**
    - **Defined scope of review:** CIAs typically require annual claims reviews and, in certain cases, arrangements reviews focused on compliance with federal healthcare program requirements, including coding, billing, and financial relationships.
    - **Data-driven methodology:** Reviews rely on randomized sampling and structured testing protocols designed to quantify error rates and identify systemic compliance issues.
    - **Error rate and extrapolation:** Where error rate thresholds are met, CIAs may require expanded sampling and extrapolating overpayments across the relevant population.
    - **Independent reporting:** IRO findings are reported directly to OIG as part of the organization's annual reporting obligations, providing external validation of compliance performance. The organization is responsible for submitting corrective actions related to IRO-identified errors in its annual report to OIG.
- IRO reviews evaluation **whether compliance controls operate effectively at scale, not just in design.**

Integration with the Compliance and Ethics Program

- IROs **operate as a mechanism for testing whether a compliance and ethics program is functioning as intended**, rather than a substitute for the program itself.

- In a typical CIA structure, the compliance function is responsible for designing controls, conducting risk assessments, and implementing monitoring activities across the enterprise. The IRO, by contrast, **serves as an independent validator, assessing whether those controls produce compliant outcomes in practice through structured, data-driven testing.**

- This is a critical distinction. OIG's CIA framework does not focus solely on whether a compliance program exists or is formally implemented, but whether it is capable of preventing, detecting, and correcting misconduct. IRO reviews are one of the primary ways for OIG to evaluate that capability, translating internal compliance activities into externally validated results.

- **The relationship between the compliance and ethics program and the IRO is dynamic.** Organizations that derive value from the IRO integrate its findings into enterprise risk management processes, including risk assessments, internal audit planning, and corrective action design. Organizations that do not take this approach often treat IRO reviews as discrete reporting obligations, limiting their impact and value.

- **The effectiveness of an IRO is determined not only by its findings, but also whether those findings drive meaningful improvements in program design, controls, and governance.**

The Role of an Outside Board Expert

The Proliferation of the Outside Board Expert

- An outside board compliance expert is an external advisor engaged to assist an organization's board in evaluating the effectiveness of the organization's compliance and ethics program and fulfilling its oversight responsibilities.
- The role is distinct from management, legal counsel, and the compliance function. Rather than designing or implementing compliance activities, the expert provides an **independent, objective assessment of whether the compliance and ethics program is functioning effectively in practice.**
- **The concept is grounded in OIG's longstanding emphasis on active, informed board oversight of compliance and ethics programs.** OIG guidance, including the General Compliance Program Guidance, makes clear that boards are expected to understand key compliance risks and evaluate whether the compliance and ethics program is capable of preventing, detecting, and correcting misconduct.
- The use of independent board compliance experts is not new; CIAs have incorporated similar roles for more than a decade, but historically these requirements were applied selectively and without a consistent or standardized approach in the years preceding 2025.
- **Recent CIAs have formalized this expectation by requiring the appointment of the outside board compliance expert.** These experts are typically tasked with reviewing the compliance and ethics program, reporting findings directly to the board, and supporting the board's ability to make informed determinations regarding program effectiveness.
- **The incorporate of an outside board expert reflects an evolution from general oversight expectations to structured, externally supported evaluation at the board level.**

The Expert's Relationship with the Board

- **The introduction of an outside board compliance expert provides an additional layer of objective evaluation focused on whether the compliance and ethics program is functioning effectively in practice.**

- Rather than participating in program design or implementation, the expert independently assesses program performance, drawing on data from risk assessments, audits, investigations, and monitoring activities to evaluate the efficacy of existing controls.

- In a CIA environment, the expert's findings are presented directly to the board and incorporated into formal reporting to OIG, **creating a structured mechanism for external validation of compliance program performance.**

- At a practical level, the expert's role is to **identify gaps, test assumptions, and assess whether the organization's compliance activities are capable of preventing, detecting, and correcting misconduct,** consistent with OIG's expectations for effective compliance and ethics programs.

- The presence of an outside expert reframes compliance oversight from reliance on internal reporting to structured, independent evaluation of program effectiveness.

Board Expert Requirements in Recent CIAs

- Two recent CIAs illustrate how OIG is formalizing the role of the outside board compliance expert.

VHS Holdings (Vohra Wound Physicians) (Effective November 20, 2025)

- Vohra's Board of Directors was required to retain an independent compliance expert within 90 days of the CIA effective date.
- The CIA mandated that the expert evaluate compliance program effectiveness at specified intervals (the 1st and 4th reporting intervals).
- OIG specified that the expert must not be employed by Vohra or have any relationships that would undermine objectivity.

Recovery Center of USA LLC (Effective May 4, 2026)

- The CIA required that Recovery Center's Board of Directors to appoint a dedicated "Board Compliance Expert" within 90 days of the CIA effective date.
- Like Vohra, the CIA mandated that the expert conduct an independent evaluation of the compliance program's effectiveness at specified intervals (the 1st and 4th reporting periods).
- The CIA further required that the expert prepare a written report of its findings, and that the Board formally review and respond to those findings, with both the expert's report and the Board's response incorporated into the organization's annual reporting to OIG.

Copyright and Disclaimer

Appendices: Agency Guidance

1. OIG
2. DOJ
3. Centers for Medicare & Medicaid Services (CMS)
4. New York State Office of the Medicaid Inspector General (OMIG)

OIG

- Collaborative Resources for Health Care Boards of Directors (AHLA, HCCA, Association of Healthcare Internal Auditors)
  - Corporate Responsibility and Corporate Compliance (2003)
  - An Integrated Approach to Corporate Compliance (2004)
  - Corporate Responsibility and Health Care Quality (2007)
  - Practical Guidance for Health Care Boards on Compliance Oversight (2015)
- Compliance Program Guidance (CPG) Documents
  - General Compliance Program Guidance (2023)
  - Nursing Facility Industry Segment-Specific Compliance Program Guidance (2024)
  - Medicare Advantage Industry Segment-Specific Compliance Program Guidance (2026)

DOJ

- Evaluation of Corporate Compliance Programs (Sept. 2024)
    - Based, in part, on the United States Sentencing Guidelines
- Memorandum on Selection of Monitors in Criminal Division Matters (Galeotti Memo) (May 2025)
    - DOJ policy on when independent compliance monitors are appropriate and how they are used to assess program effectiveness
- Increasingly, agencies announce their policy intentions in public addresses:
    - Deputy Attorney General Todd Blanche delivered remarks at the 2025 ACI Foreign Corrupt Practices Act and Global Anti-Corruption Conference outlining DOJ's priorities and announcing a forthcoming DOJ-wide corporate enforcement policy (Dec. 2025).
    - Principal Deputy Assistant Attorney General Matthew R. Galeotti delivered remarks at the SIFMA Anti-Money Laundering and Financial Crimes Conference addressing corporate compliance policy and enforcement expectations (May 2025)

CMS

- Conditions of Participation: Governing Body (42 CFR § 482.12)
- Compliance Program Guidance for Medicare Fee-for-Service Contractors (2005)
- Patient Protection and Affordable Care Act (2010)
    - Providers and suppliers required to develop compliance programs as a Condition of Participation in the Medicare Program
- Compliance Program Guidelines for Medicare Advantage Organizations and Prescription Drug Plan Sponsors (2012)

OMIG

- OMIG Provider Compliance Manual (2023)
- Compliance Program Review Module (2023)
- Compliance Program Self-Assessment Form
- Compliance Program Requirements FAQs (2023)