

A BOARD PERSPECTIVE

Where Compliance Belongs

Why the compliance program should sit within Legal—and how artificial intelligence will make it leaner over time

Compliance is not a separate kingdom. It is the engine that turns Legal's judgment into action—best placed inside Legal, where privilege, expertise, and budget already live, and where **AI will do more of the work each year.**

Legal vs. Compliance

Two distinct jobs—which is exactly why they belong under one roof

LEGAL

“What should we do?”

- Interprets the law and chooses reasonable, defensible positions.
- Advises and advocates for the company; owns legal judgment.
- Licensed attorneys with professional duties and privilege.

COMPLIANCE

“How should we do it?”

- Manages the people, processes, and systems that address risk.
- Prevents, detects, and responds—does not interpret the law.
- Often non-lawyers; no independent professional duty to the company.

Three Common Reporting Models

Where companies place compliance—and which model predominates

MODEL 1

Within Legal

Compliance reports to the Chief Legal Officer as a function of Legal.

Predominant for non-regulated companies

MODEL 2

Within Risk / Finance

Compliance sits in enterprise risk and reports to a Chief Risk Officer.

Common in financial institutions

MODEL 3

Standalone to CEO

An independent compliance function reports directly to the CEO.

Mandated in parts of healthcare

Why Compliance Should Sit Within Legal

For most companies, one roof is stronger, cheaper, and better protected

Privilege protection

With compliance under counsel, sensitive work is more readily “at the direction of counsel,” strengthening attorney-client privilege.

Shared expertise

Legal already tracks the regulatory landscape and future developments, and can feed them straight into the program.

One budget, no duplication

A single organization avoids overlapping risk assessments, training, and third-party management—and shared career ladders lift morale.

Endorsed by guidance

The SEC and a 2003 ABA task force support Legal’s primary role in maintaining an effective compliance program.

What the Guidance Actually Requires

No regulator mandates a reporting line outside a few regulated industries

- **The Sentencing Guidelines.** Chapter Eight sets the seven elements of an effective program but mandates no organizational design—effectiveness turns on culture and leadership, not reporting lines.
- **The DOJ.** Its compliance-program evaluation asks about the function’s stature, resources, and reporting line—not where the box sits on the chart.
- **The throughline.** Guidance favors separating compliance from the business it oversees—never from Legal.

THE BOTTOM LINE

An effective program depends on culture and leadership—*not on the org chart.*

The Regulated Exceptions

Two industries where regulators push compliance outside Legal

Healthcare

Health regulators direct that compliance, legal, and audit remain separate functions—and settlements often mandate a compliance officer reporting to the CEO.

Separation by mandate

Financial Services

Banking's "three lines of defense" places compliance in independent risk management, typically reporting to a Chief Risk Officer.

Control-and-monitoring model

Outside these regulated spaces, companies rely on the general guidance—and overwhelmingly keep compliance within Legal.

What the Fortune 100 Actually Do

Public disclosures point overwhelmingly to compliance within Legal

Nearly all

of large companies place
compliance within or reporting
through Legal

Every

Fortune 100 names its Chief
Legal Officer to the senior
leadership team

Just one

Fortune 100 company
discloses its Chief
Compliance Officer as a
named executive officer

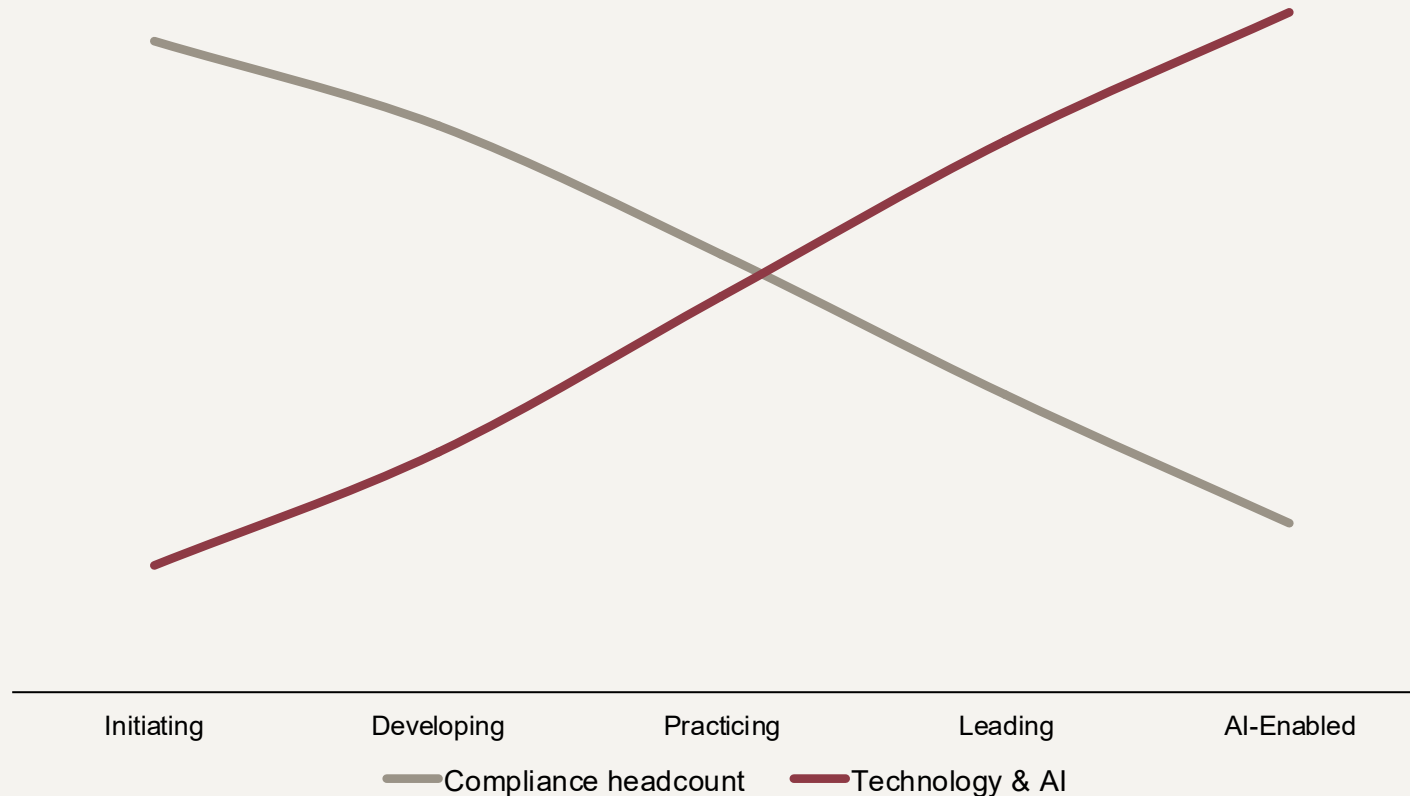
Rare

standalone compliance
organizations outside
regulated industries

The market has voted: boards consistently treat the Chief Legal Officer as a top officer, while compliance sits within or beneath Legal rather than standing alone.

AI Will Make Compliance Leaner

As programs mature and AI advances, technology rises while headcount falls



WHY IT HAPPENS

- **Tasks automate.** Data management, risk assessment, training, and routine subject-matter guidance are increasingly handled by software.
- **AI compounds it.** Models can answer compliance questions across hundreds of jurisdictions and learn from prior use.
- **Lawyers remain.** Independent legal judgment by licensed professionals cannot be automated away.

What This Means for the Board

Five questions to guide how the program is placed and resourced

Keep compliance close to Legal

For most non-regulated companies, reporting through the CLO maximizes privilege, expertise, and efficiency.

Invest in technology and AI

Fund the tools that automate routine compliance work before adding headcount.

Right-size as automation matures

Expect the human footprint to shrink as the program matures—plan for it deliberately.

Guard against silos

Whatever the structure, ensure compliance stays connected to enterprise risk and to leadership.