

# Best Practices for CEOs to Build Compliant Organizations

Article By:

Robert J. Herrington

---

A **strong correlation exists between corporate compliance and positive financial performance**, and business leaders are taking note. While some might see “compliance” as a regulatory-laden burden for companies, the more evolved and successful CEOs see compliance requirements as an opportunity to hardwire corporate goals, risk management and smart, efficient processes into their firm’s DNA.

CEOs must, can and should strive to build compliant organizations for the traditional reasons of avoiding civil or criminal prosecution by regulators, as well as avoiding the potentially massive financial exposure and media embarrassment that often follows a compliance misstep. Further, there is nothing so repulsive to a C-suite chief as paying millions to a plaintiff’s class action firm for legal fees and tens of millions more to their clients because the company failed in some basic compliance duty.

In researching my book ***Verdict for the Defense*** (Sutton Hart 2011), as well as in my mass action defense work, I have discovered that the one of the best defenses to the jackpot justice that often puts a target on America’s leading companies is to put on a proactive offense, and an important element of that offense is regulatory compliance. Also, I have learned that compliance is much more than a million-dollar software program. True compliance is as much a corporate attitude that comes from the top; it begins as CEOs learn that compliance is tied to increased profits and improved financial performance.

According to a recent study conducted by University of Pennsylvania’s Wharton School, there is a positive relationship between an organization’s risk management framework and its financial performance. The study developed a “risk maturity index,” which assesses factors like the board’s understanding of and commitment to compliance and risk management; executive level responsibility for risk management; creating a corporate culture of risk engagement; and accountability and formal processes for identifying, assessing and mitigating risk. The study found that higher risk maturity rates are directly associated with improved return on assets and stock performance.

So, if we accept that compliant organizations with a robust risk management framework benefit from better financial performance, the question becomes exactly how a CEO can drive this mission-critical goal. In my own research and experience helping company leaders manage their risk management and compliance duties, I have identified several best practices that apply to a broad spectrum of companies and generally are present in every consistently compliant (and successful) business entity.

---

Here are the top five best practices for your consideration:

## **Board and Management Commitment**

Your firm has little hope of becoming a compliant organization absent a commitment from the top. The board and senior management must be (in perception and reality) driving compliance and risk management efforts by word, political will and allocation of resources.

## **Clear Statement of Risk Management and Compliance Goals**

Here is the area where the CEO can have the most impact. I propose that CEOs adopt a no-tolerance policy for compliance irregularities, problems and the litigation that frequently ensues. Although there always will be exceptions, compliance issues and litigation can and should be just that – the exception.

When problems almost or actually occur in this area, it means something went wrong. The cause of those failures must be identified, analyzed and rectified, and those responsible held accountable.

But is mere “compliance” enough? Rarely. Consumer protection laws in many states give plaintiffs’ lawyers tremendous leeway to argue that a practice is misleading or unlawful, even when a company’s conduct technically complies with regulatory requirements. And this is where class action lawyers make their bountiful living, in the grey areas of compliance and regulatory requirements.

**Corporate heads should adopt a “compliance plus” goal, where organizations steer clear of grey areas and potentially questionable conduct** and focus on using compliance as a starting point in the process and thereby drive the value derived from a compliant organization.

## **Executive-level Responsibility**

Board and management-level commitment to compliance is essential, but not enough. Achieving compliant organization status takes political will and the necessary allocation of resources – both of which require executive-level involvement and responsibility.

Financial performance is simply a measure of how much of what your company brings in that it gets to keep. Since executive-level officers are responsible for what you bring in, there is no reason they should not also be responsible for the second half of the equation, ensuring that the company gets to keep as much as possible.

## **Align Compensation and Incentives to Compliance Goals**

This best practice scenario is best illustrated by example. If you have an executive who develops a new product or marketing campaign that grows company revenues by \$10 million in year one, but that initiative results in compliance problems and litigation costing \$15 million over years two, three and four, how should that executive be judged? If company policy rewards that person for revenues alone without regard to the attendant costs, your company will never reach its compliance goals.

## **Establish a Comprehensive Risk Management and Compliance Framework**

Board-level commitment, clear goals, and properly incentivized executive-level responsibility are prerequisites, but they will mean little without a comprehensive framework for identifying, assessing, mitigating, and monitoring risk and compliance issues.

Compliance problems are not simply “an issue for the legal department.” Unless your company has a comprehensive framework that involves compliance and risk mitigation experts at each level of your organization’s business processes, from product development and design, to marketing, customer service and complaint management, risk mitigation and compliance efforts will become reactive and isolated, unable to prevent problems before they occur.

©2025 Greenberg Traurig, LLP. All rights reserved.

---

National Law Review, Volume I, Number 330

Source URL: <https://natlawreview.com/article/best-practices-ceos-to-build-compliant-organizations>