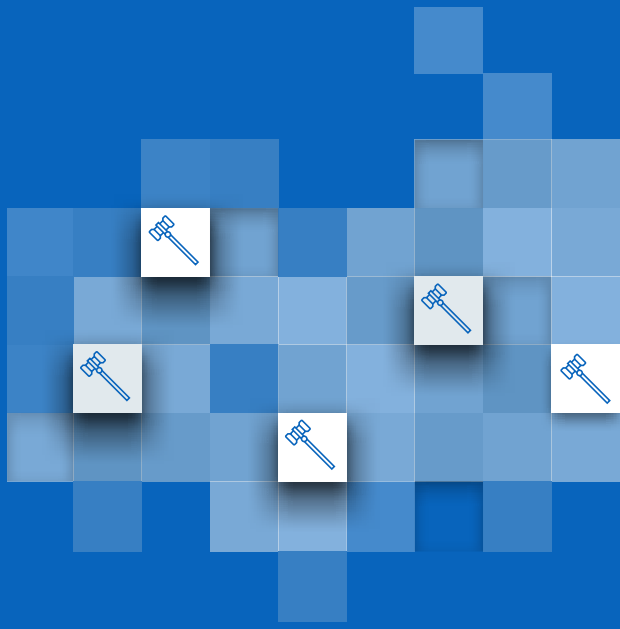
How The C-Suite is Blinded by Compartmentalized Compliance Efforts

Brian Rizman, Edgile Managing Director



Many enterprises today are losing the battle to maintain compliance and it's frighteningly unintentional. These companies have senior executives who believe—incorrectly—that managers are tracking and managing all of the company's compliance obligations. The truth is that these firms have compliance matters so compartmentalized by business units and specialty that critical compliance requirements routinely fall through the proverbial cracks.

The solution?

Have one senior manager or executive responsible for all of the enterprise's compliance and regulatory needs, so that nothing inadvertently gets hidden from view.

Siloed compliance management creates problems

Within many enterprises today, compliance and regulations are often managed in silos. For example, issues that are seen as primarily dealing with technology—think ISO or PCI—are handled by IT and ultimately the CIO, whereas those seen primarily as financial—such as SOX or FCPA—are dealt with through finance and treasury, the controller's office or the CFO's team. Sometimes regulations are handled by internal audit or legal teams or the Chief Risk Officer, but unless someone bothers to ask, actual ownership may not be obvious.

Allowing specialists to handle rules in their arenas is understandable. But there are two massive problems with this approach.

The first is that few regulatory requirements exist solely within any one group's jurisdiction. Take PCI. Is that regulation primarily technology-driven and in IT’s purview, or is it primarily security-driven and more under the

> “Many enterprises—depending on operational geographies, verticals and various other factors—must deal with well over 100 regulations.”
>
> - Brian Rizman, Edgile Managing Director

auspices of the CISO/CSO? For that matter, what about the privacy aspects (think GDPR or the California Consumer Privacy Act) within PCI? Should the Data Privacy Officer or some other entity take the lead? The reality is that many of today's rules are sufficiently comprehensive that they touch on many groups.

The far bigger problem is that such compartmentalization efforts make it likely that some requirements will get missed. Each responsible manager may assume that someone else is handling a new requirement when in fact no one is. That's why it's essential to have one person who oversees compliance and regulations across the organization.

Two problems with allowing specialists to handle rules in their arenas:

1. Few regulatory requirements exist solely within any one group’s jurisdiction
2. Compartmentalization efforts makes it likely that requirements will get missed

Looking at compliance obligations holistically

Many enterprises—depending on operational geographies, verticals and various other factors—must deal with well over 100 regulations. With a centralized executive in charge, the opportunity exists to look at compliance obligations holistically.

There are regulations that are critically germane and some that are viewed by senior management as more peripheral and less of a priority. The lower priority rules are the ones most likely to be neglected and to subsequently deliver painful surprises. It's one thing for senior management to review certain requirements and make a strategic decision that the cost of compliance for those rules isn't worth it. But it's quite another for the enterprise to be blindsided by penalties for regulations that senior management thought—incorrectly—someone on the team was already handling.

The board needs to appoint a single executive who is responsible for triaging every regulatory requirement—local, state, federal, global, industry—and deciding what the firm will and won't do in each case. This person certainly can—and should—dole out assignments to various specialized departments as needed. But with one person tracking all obligations, there is less opportunity for missed or overlapping initiatives. Don't forget that the compliance landscape continually changes. As a company moves into and out of different markets and different geographies, the rules that have to be tracked evolve. Individual regulations also change

regularly. With more than a hundred sets of rules for the typical enterprise, tracking changes alone can be a full-time responsibility. Then there are new rules cropping up all the time. The European Union's GDPR and the California Consumer Privacy Act are just two examples of 2018 rules that weren't causing organizations a challenge a year earlier.

Avoiding duplicative GRC efforts and expenditures

When a company isn't comprehensively tracking its compliance landscape due to siloed efforts, being exposed to unexpected fines and penalties is far from the only pain point. It invariably results in the company making investments in overlapping and duplicative Governance, Risk and Compliance (GRC)-related technologies. This results in a lack of coordinated efficiencies and likely overpaying for licensing fees, hardware costs, cloud costs, and unnecessary labor resources. The GRC tool overlapping problem can get worse every time there's an acquisition, because a new company may bring in its own tools that no one feels comfortable jettisoning.

What's needed are triggers to re-evaluate the compliance landscape. When a company explores any corporate change, such as a merger, acquisition, divestiture, or entering or leaving a vertical or geography, someone needs to investigate all of the potential compliance implications and make sure they are understood by senior management before the business decision is made. Otherwise, the cost of that corporate change might be quite a bit higher than the CEO and board thought when the move was approved. ROI and TCO calculations are not just for product purchases.

I have been making the argument that you need to create a centralized compliance executive position, with jurisdiction over all operations. Whether you create such a post—or add those duties to an existing post—it's essential that this person have a dotted-line relationship with every single relevant department, including audit, security, IT, finance and treasury, human resources, and more. This centralized risk management executive must also own all GRC activities and, ideally, report directly to the board and the CEO.

Whereas COOs are, in theory, managing day-to-day operations of the company, CEOs tend to focus their energies and attention on different units from day-to-day, depending on where the chief executive sees the greatest need. But board members are much freer to maintain the big-picture perspective, which is why it's so important for the board to hear directly from this compliance overseer.