Complicated operations: spot the compliance gap?

Invisible to the eye

Compliance risks rarely present themselves at the surface, warns **EisnerAmper** audit partner **Dov Braun**. Accordingly, CCOs must recruit their colleagues, who can have a deeper understanding of the compliance risks in their respective fields, to discover where the problem areas rest

Picture the CCO, diligently scanning his morning emails for signs of trouble. With a raised eyebrow, he clicks on a link opening the transcript of an US Securities and Exchange Commission (SEC) official's speech, who the night prior warned that private equity expense allocations are becoming a priority area for inspectors. Further down his inbox, he notices a number of client alerts from law firms, all reacting to the speech with words of caution. It sticks with him all afternoon.

The CCO, of course, gets it. The firm's policies and procedures on fees and expenses, including how they are disclosed and allocated between investors and the management firm, need to be carefully reviewed and most likely updated. From here on out, every receipt requires thoughtful judgment – anything less opens the firm to SEC enforcement action.

Simple, right?

Here's the problem: how does the CCO instill that same level of urgency across the firm? Sure he or she may have devoted a morning to reading about fees and expenses, but everyone else was busy worrying about their own job responsibilities.

Dov Braun, who provides accounting and auditing services to private fund managers including real estate and private equity, makes the observation with a deep appreciation for the challenges faced by compliance chiefs.

"We talk a lot about creating a culture of compliance. What it means is the controller has just as much appreciation for policy and procedure when they allocate a simple plane ticket receipt as would the CCO," says Braun, who practices from the New York office of EisnerAmper, a consulting and accountancy firm.

> "A lot of times compliance folk are kept out of the loop, but they need to have a broad overview of everything going on at the firm"

"And that requires the CCO have a seat at the table. A lot of times compliance folk are kept out of the loop, but they need to have a broad overview of everything going on at the firm. That means having a presence with the operational group, the portfolio management group, the marketing group and so on."

Braun says that a CCO "who isn't in the know" will have a hard time getting his or her message across. Worse still, it becomes difficult for the CCO to develop an in-depth understanding of the various operations and functions constituting the firm's governance, each of which comes with its own unique set of compliance risks. But how does a CCO know when they are embedded enough? Braun says it starts with having the right playbook.

A roadmap that works

"It's one thing to have a playbook or right framework that provides a good risk profile of the firm, but it's quite another to see that your playbook is working as it should," says Braun.

He says that CCOs will often have all the right pieces (i.e., high-level compliance risks identified) but fail to arrange them in a way that ensures all the right people are part of the compliance

strategy. When they do, the CCO invariably becomes a visible presence in all areas of the firm.

"The easiest example to think of is a significant change in business. A firm that's growing, and may be entering into new areas of business, will have new types of conflicts of interests to consider. The CCO may have these mapped out, but the challenge is working through how those risk areas touch upon different people through a chain of action," says Braun. "If the firm is embarking on a new debt strategy, sit down with the deal guys and work through how an equity investment works versus a debt investment."

As part of his work, Braun performs forensic testing on GPs' workflow management processes with the specific aim of identifying compliance weaknesses. "Any time you have a specific conflict of interest, you can, for instance, create a reporting mechanism to the CCO."

The other thing is to "review yourself," says Braun. Even with the best roadmap of the firm's principal compliance risk areas, a CCO needs to be able to test their own review processes and document them.

"A common mistake CCOs make is not monitoring and adjusting for risk enough. Operations are fluid, and change is frequent. Working from a stale compliance playbook can lead to mistakes," says Braun.

He points to cybersecurity as a prime example of where best practices are in need of an update. As part of their due diligence on third-party vendors, more GPs are asking questions about the protection of their data, but even in the last six months the safest firms are extending those same questionnaires and data security requirements to subcontractors of the third-party vendors. "Better yet, do an on-site visit of the third party vendor and document the meeting," says Braun. "GPs will file answers to the questionnaires but not keep in their records how those meetings went for review purposes."

Braun: bad compliance equals bad operations

Whatever compliance playbook the firm is working off of, another important element is buy-in from all members of the firm. Braun says a CCO's voice creates more of an imprint when staff understand the rationale behind a new compliance policy.

Designed to prevent wheeling and dealing, the SEC's "pay-to-play rule," for instance, limits a fund manager's ability to make political contributions. Instead of just imposing a strict ban on political donations, it's wiser for senior management to provide some color, says Braun. "Have them appreciate the need for the rule. Explain that giving money to a campaign can jeopardize the firm's business with a key LP."

The CCO's job is too vast and complex to handle alone, Braun concludes. Fortunately, with the right messaging and training (as well as a little help from outside consultants), they can harness their colleagues' collective experience and intelligence to pinpoint compliance weak points in the firm's operations. ■

Risk all around

Operational risk, of course, goes beyond the lens of compliance. Braun says that IT is another major area where poor execution can disrupt the firm's ability to conduct business.

"GPs need the latest technology to keep pace with investor demands and manage their increasing workloads but don't always make the right moves when implementing new systems."

He says one common mistake firms commit is not making sure all the right access controls (so certain information is only accessible to who it should be) are kept in place when migrating to a new IT system.

Another common mistake when trying out new software is not keeping a log of when problems arise. Braun says having a record of glitches and undesired system outcomes allows the IT department to retest known problem areas after a system upgrade as a way to test for improvement.

Scheduling a "redundancy phase," in which an old system runs in parallel with the new system, is another best practice, says Braun. "I've seen some clients let their old tech contracts expire only to have to scramble when they realize the new system couldn't handle a certain task."