IGNITES

As Regulators Dive Deeper Into Data, Shops Sharpen Chops

By Jill Gregorie December 12, 2017

As regulators rely more and more on tech tools to detect violations and potential weaknesses in fund shops' compliance programs, CCOs and their teams are focused attaining the programs and skills needed to aggregate and analyze data.

In fact, results of a July 2017 *Ignites Research* report show that more than six in 10 compliance leaders cite improving their department's use of data in compliance tasks over the next two years as a top priority, and a precursor to being viewed as someone who drives strategy within their organizations.

The survey captured responses from chief compliance officers, deputy CCOs and general counsel at 32 U.S. fund companies that as of the end of May collectively managed $900 billion in long-term mutual fund and ETF assets.

The SEC's continued investment in tools and instruments that mine data to spot irregularities and potential regulatory violations is in part driving compliance officers' urge to become more tech-minded, says Maria Gattuso, Deloitte's lead regulatory advisory principal in the investment management industry.

"When you have a regulator that has increased their capabilities, and as a firm, you're subject to that regulator, you feel you ought to be doing the same thing and knowing what story you're telling a regulator," she says.

In addition, CCOs who can map out data in easy-to-understand charts and tables can better pitch ideas to senior management, she says. But many lack the tools and technology that can help them do so, Gattuso says.

"If you could take a compliance person who knows all the regulations and the compliance items that the firm needs to comply with, and combine that with a data scientist who can cull through data and do data analysis, you'd have the perfect person," she says.

Such a professional, however, "does not exist" at fund providers today, she says.

Beyond acquiring technological resources, compliance staff need to earn the trust of other departments that may see the compliance team as the office cops.

“It can be an uphill battle trying to get people to cooperate,” says Janaya Moscony, president and founder of SEC Compliance Consultants.

“There definitely is a struggle” in trying to obtain data from IT or service providers, especially for staffers who may be asking for data that had traditionally never been shared with compliance before, she notes.

That makes securing buy-in from executives who may need to sign off on their access to certain systems and the business units that manage the data a critical first step.

Explaining the rationale for the data request, and reiterating that the CCO has the backing of senior management, can help others become more comfortable sharing information, Moscony says.

Compliance should also ask members of the C-suite to emphasize that each department needs to verify their data reports as complete and accurate before storing it in a warehouse or sharing it, so that compliance officers don’t waste time redoing it, says Samer Ojjeh, principal and asset management advisory leader at EY.

Even with such verifications, teams would need to spot-check the data to verify that it has been scrubbed and validated, and oftentimes a visual scan is sufficient to tell whether data has been compiled properly, Deloitte’s Gattuso says.

“Your analytics are only as good as your data,” she says.

Firms can also help compliance by hiring technologists or business analysts to help document where data is stored, and create systems that automate searches and aggregate reports, says Whitfield Athey, CEO of **Delta Data**.

Fund companies should also consider creating systems that aggregate all the data compliance officers seek from various departments in order to provide a firmwide perspective, he says. Collecting silos of data from departments and analyzing them separately leaves plenty of room for error or missed patterns, he says.

In the meantime, compliance needs to learn how to get the data they need using the systems that their shops already use, Athey says.

“People in compliance today should allocate as much of their teams’ time as possible to documenting where data comes from, who owns the data, with what frequency can they get the data and how that all fits into their reporting structure,” he says.

Once compliance officers learn how to gather this information, they should work to “slice and dice” transactional-level data, which is where compliance violations — intentional or otherwise — most often occur, says Amy Lynch, founder and president of FrontLine Compliance.

Although many compliance officers “look at a trade blotter like it’s ancient Greek,” they should be able to analyze trading activity patterns and confirm that those fit in the limits placed on the fund’s investments, she says. “Compliance, in my opinion, needs to be as smart as portfolio managers.”

Software can help to scrutinize such activity.

“The advancements in data analytics and the user-friendly nature of these tools have allowed business users to be able to be more effective in managing data themselves, instead of relying on IT to generate reports,” EY’s Ojjeh says.

One caveat is that compliance will still need to carefully look over exception reports, and when necessary, go back to the raw data to look for potential red flags manually, FrontLine’s Lynch says.

Regular testing of such systems is another important factor.

“It’s one thing to have it set up and running, but compliance staff needs to have a comfort level in knowing the system is working as intended,” Lynch says.

“The biggest mistake firms make is setting it and forgetting it,” she says.