CEP Magazine - April 2020
Developing a data analytics-enabled compliance program for the real world

By Matt Reeder and John Kim

Matt Reeder (mtreeder@orrick.com) is an Associate with Orrick Herrington & Sutcliffe LLP in Washington, DC.
John Kim (john.kim@controlrisks.com) is a Director with Control Risks in Washington, DC.

This is the first article in a two-part series.

In a speech at the Government Enforcement Institute in September 2019,[1] Deputy Assistant Attorney General Matthew Miner raised a few eyebrows when he said that Department of Justice (DOJ) lawyers would scrutinize whether and how a potential enforcement target used data analytics to "analyze or track its own data resources—both at the time of the misconduct, as well as at the time [DOJ is] considering a potential resolution." On their face, these comments were most directly targeting "compliance-oriented companies in the securities and commodities trading space," but they came near the end of his remarks describing the broader efforts of DOJ's Fraud section. Miner acknowledged that "the subject [of data analytics] doesn't fit as well with the other aspects of these remarks." However, he insisted "the topic actually does fit thematically."

As a term in the compliance industry, "data analytics" often serves as a catchall to include anything remotely related to technology. The phrase is often overused and unclear. Data analytics is often categorized alongside other technology jargon like "cloud," "big data," and "AI."

So how must compliance professionals respond to Miner's remarks?

Today, companies gather, create, and store ever-increasing amounts of data so they can anticipate and act quickly on fleeting business opportunities. Regulatory bodies seem to expect improved compliance programs as corollaries to these data-enhanced business practices. Regulatory and enforcement bodies expect companies to cultivate data analytics capabilities to identify misconduct and then to mitigate the misconduct by analyzing and tracking their internal data resources. These expectations will likely become requirements—either through practice, by rule, or by law—and companies will be required to implement proactive technology-enabled measures to detect and analyze fraud, abuse, and misconduct before they become endemic.