Bridget Johnson (bejohnson@bdo.com) is a Manager at BDO, based in Washington, DC, USA.

Corey Dunbar (cdunbar@bdo.com) is a Principal at BDO and the leader of BDO's Data Forensics service line, based in New Jersey, USA.

Morgan Dalton (mdalton@bdo.com) is a Senior Associate at BDO, based in Washington, DC, USA.

What makes an effective compliance analytics program?

By Bridget Johnson, Corey Dunbar, and Morgan Dalton

Data analytics disrupted just about every business function, and compliance is no exception. Over the past decade, forward-thinking compliance officers were early adopters of incorporating data analytics into their compliance programs. In recent years, however, data analytics evolved beyond "nice-to-have" into a nonnegotiable component of an effective compliance strategy.

For those not yet convinced, just look at the United States Department of Justice's (DOJ) June 2020 guidance, which states an effective compliance program is based on "continuous access to operational data" instead of assessing risk from a snapshot in time.[1] Practically speaking, companies cannot meet DOJ's expectations for real-time transaction monitoring without leveraging data analytics.

But what does an effective implementation of compliance analytics look like? This article explores five differentiators of well-designed compliance analytics programs, offering guiding principles for companies to consider when developing or enhancing their compliance analytics strategy (see Figure 1).

Figure 1: Five elements of an effective compliance analytics program

Elements of an Effective Compliance Analytics Program

- It's Proactive
- It's Holistic
- It's Tailored
- It's Dynamic
- It Delivers

It's proactive

It's no secret that regulators such as DOJ and Securities and Exchange Commission (SEC) are using data analytics to proactively mine data to identify potential misconduct and behavior in violation of legislation. To keep pace, companies must do the same. Many businesses wait to employ data analytics until there is an investigation, which is a major misstep. Yes, data analytics is an invaluable investigative tool, but the beauty of analytics is that it unlocks a real-time view of a business's operations and risks. To maximize the power of analytics, companies should proactively incorporate analytics and technology more broadly into their compliance programs to identify anomalous behavior, determine the associated risk, and develop a remediation plan before regulators do.

To be most proactive, it is best practice to employ analytics at the initial risk-assessment phase of the compliance program. Risk assessments have historically followed a heavily qualitative approach. While qualitative reasoning is essential in assessing risk, it does not paint the whole picture. It is crucial for a company to inspect its underlying data—such as sales, procurement, expenses, communications, and employee data sets—to achieve the most factual understanding of its operations and risk profile. Companies should also focus on risk mitigation efforts, such as compliance policies and monitoring procedures.

For example, imagine a company is assessing its Foreign Corrupt Practices Act (FCPA) risk. It has general knowledge that it interacts with politically exposed persons (PEP), but it does not have a clear idea of which parts of the business are most at risk. Using data analytics, the company could analyze its business partners to identify specific segments or geographies of its business that most frequently interact with PEP and therefore have the highest FCPA risk. With this information under its belt, the company can make informed decisions on adjusting its compliance policies for those business areas, and where to focus its transaction monitoring.

This document is only available to members. Please log in or become a member.

Become a Member Login