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.

In order to build a technology-enabled compliance program, companies should first internally assess the tools currently available to them, and then determine what they must implement—either in-house or off-the-shelf.

In this two-part series, we will discuss how compliance programs can become technology- and data-ready to improve outcomes, prevent misconduct, and withstand government scrutiny. Not all compliance departments can access and unlock a company's data and technology resources. Such compliance programs are in the pre-maturation phase. This article will offer advice to pre-maturation phase companies and suggest steps to begin building out a technology- and data analytics–enabled compliance program to perform effectively and cost-efficiently. A company enters the post-maturation phase once it gains capabilities to access and unlock data and technology. In part two of this article, we will discuss considerations important to building a proactive compliance monitoring solution in the post-maturation phase.

Companies with a still-maturing data analytics program should proceed in three steps.

Step 1: Assess established procedures, capabilities, and tools

Companies often undertake improving their data analytics programs without a strong sense of where to begin or how to incorporate data analytics into their already-existing programs. Too often, vendors tout their ability to automate workflows and develop artificial intelligence to "let the machine handle everything." While these goals are admirable, and in some cases achievable, integrating technological and data analytics–based solutions is not instantaneous. Data analytics is not a panacea; it is a constantly evolving array of tools that support and enhance (but do not replace) compliance functions. The best approach, therefore, is the incremental solution. The compliance program must mature into the use of data-based tools.

Companies should look internally to assess what established procedures and current capabilities exist to seek out weaknesses and deficiencies. Before companies even begin to understand their technology and data gaps, they should first focus on understanding their skills and personnel gaps. A state-of-the-art, technology-enabled compliance program is only as good as the people reviewing and analyzing the results. Corrective action remains in the hands of compliance professionals. These compliance professionals must commit to data literacy to properly interpret the computer-generated analytics results.

Assessing established procedures and current capabilities can identify pre-established skills and tools within the company. Understanding what is already at their disposal will allow compliance professionals to leverage and co-opt existing in-house processes more efficiently and cost effectively.

Assessment questions

- What type of program is currently in place, and how technology-enabled is the program?
- What types of tools are already in place?
- Can this be developed internally?
- Who and what comprise the IT resources that can help us answer these questions?
- Does anyone in the compliance department already work with data and understand technology?
- How do we envision our compliance professionals using data?
- How does the collection, retention, and use of data overlay onto the applicable legal and regulatory framework?

Step 2: Inventory systems, create data maps, and identify shortfalls

Compliance professionals often have vast stores of internal data with which to build an effective proactive monitoring program. For example, vendor and employee information from enterprise resource planning (ERP) systems can be proactively scanned to identify potential conflicts of interest. Statistical analyses on financial transactional systems can provide insight into misappropriation. Sentiment analyses and keyword detection can flag potential bad actors before misbehavior occurs. However, without understanding the variety and scope of existing data sets, it is impossible to leverage that data with technological or data analytics tools.

Compliance professionals should collaborate with their IT team and other departments to inventory and catalog data systems and create data maps. IT teams can provide a system infrastructure map detailing the data resources at the company's disposal. Other departments can deepen the compliance function's understanding of each data resource. For example, the accounting department can offer insight into how it uses accounts payable and accounts receivable data; human resources can provide insight into employee information, expenses, etc.

Only after properly inventorying and cataloging data resources can compliance professionals begin to identify shortfalls and weaknesses in their current infrastructure. These shortfalls and weaknesses can take varied forms, like gaps in the data that make historic norms impossible to establish or a lack of system-wide technical controls.

Compliance professionals should work with all data stakeholders (IT and other departments) to analyze their catalog and maps of company data to specifically identify shortfalls and weaknesses and then build a development plan.

Assessment questions

- What ERP systems and financial systems are currently in place?
- Where do these systems reside?
- What technical controls are currently in place?
- What policy controls are currently in place?
- How do we currently respond to suspicious transactions?
- Does a system of alerts and reports for suspicious transactions exist?

Step 3: Develop a data-enabled plan to shore up shortfalls

Building an effective technology- and data analytics–enabled compliance program requires enterprise-level collaboration and input. Compliance professionals must communicate data needs to their IT team and work with them to understand the technical requirements of meeting those needs. Each affected department must buy in to the notion that proactive compliance measures will improve their business practices. However, this does not mean that a large-scale development plan should be presented at once.

Bureaucratic inertia is real and has been the downfall of many a large-scale development plan. As with any change, improved compliance practices must be affected incrementally. Compliance professionals should categorize and organize their incremental development plans based on areas of need, criticality, and impact. Such development plans are more likely to garner needed support across the company and to remain nimble enough to adapt and evolve with changing circumstances.

After beginning incremental development, compliance offices can begin implementing data analytics into their compliance workflows.

Assessment questions

- What do we need to close identified gaps?
- What are the most critical areas of need based on impact?
- What are the existing solutions in the marketplace?
- What is our budget?
- How do we future-proof this?

Conclusion

An effective technology- and data analytics–enabled compliance program requires methodical and strategically focused planning. An incremental build-out is more likely to garner needed input and assistance from internal stakeholders than a wholesale change. Patience during this process is often rewarded with lasting improvements.

The three-step method for assessing and improving a pre-maturation compliance program will prepare a company to better integrate data sets and establish a holistic approach to proactive compliance monitoring. In part two of this series, we will discuss specific steps that post-maturation companies can take to improve and build on their proactive compliance monitoring programs. Such companies hold promise for developing data-literate compliance professionals who are empowered to act with creativity and to innovate in devising systems and methods for identifying and stopping breaches before they inflict serious harm.

Takeaways

- Regulatory and enforcement agencies increasingly expect data analytics–enabled compliance functions.
- Well-used data analytics can improve outcomes, predict (and sometimes prevent) misconduct, and withstand government scrutiny.
- Companies with a still-maturing data analytics programs should assess existing procedures, capabilities, tools, and resources in light of applicable legal and regulatory schemes.
- Compliance should also inventory data systems, create data maps, and identify shortfalls and weaknesses, as well as focus technology development efforts on improving identifiable weaknesses.
- Proceed incrementally to build upon existing data analytics capabilities.

[1] The University of Texas School of Law, 6th Annual Government Enforcement Institute, September 2019, http://bit.ly/383cdf0.