COSMOS
Navigate the Compliance Universe

CEP Magazine - November 2022

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

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.

It's holistic

To be most effective, a compliance analytics monitoring solution should be holistic, meaning it is built upon data from multiple functional areas of the business and augmented by less obvious data sources (such as unstructured and third-party data) where appropriate. Compliance risks exist in all business areas, and a good compliance analytics program will take that into account.

As part of designing a monitoring mechanism, a company should conduct a data assessment, which is the process of taking inventory of, mapping, and rating data sources based on completeness, accuracy, and usability. Most companies use a multitude of IT systems across different departments and locations. When scoping a compliance analytics program, it is important to consider data across these systems so that no part of the business is overlooked.

The assessment should also include unstructured data sources or data not displayed neatly in rows and columns, such as invoices or emails. These days, many tools can efficiently and systematically convert this unstructured data into a structured format, adding another potential data source to be mined for compliance risk. If unstructured data sources cannot be converted, the additional information contained in such data sources may also provide helpful context for assessing a company's compliance risk along with the structured data sources.

Many companies choose to further enrich their compliance monitoring by integrating third-party data sources into their analytics. For example, country corruption indices can be incorporated into a red flag test to identify transactions in high-risk countries, or aggregated government-sanctioned party lists can be screened against a company's customers, banks, suppliers, and other third parties. Taken together, these data sources offer a wealth of information that can be analyzed for fraud, corruption, or other noncompliant activity.

It's tailored

There is no "one-size-fits-all" approach to compliance analytics. This is because companies vary dramatically in size, location, regulations, and policies—therefore, each company has unique risks. Applying a turnkey compliance analytics program to an idiosyncratic business will result in a large volume of false positives, consuming a lot of review time. Tailoring a company's analytics to its unique circumstances and using a risk-based approach will ensure the compliance analytics solution is most effective at accurately identifying the narrow population of interest.

A risk-based approach aims to provide the right amount of information without undue burden. Put differently, instead of diving deep into every element of a company's data, a more effective strategy is determining which

information or data requires more attention as the potentially higher risk and focus there. Compliance analytics helps companies achieve this by narrowing their entire enterprise data universe (typically in the hundreds of terabytes) down to specific line items, relationships, entities, or behaviors that require human review.

A best practice in this area is to anchor a company's compliance analytics strategy to the outputs of its risk assessment and data assessment exercises, focusing on the intersection of elevated risk and available data. For instance, if a company's highest risk point is its payments data, but the payment data is not complete or contains quite a few errors, a good compliance program focus will be to ensure the data quality is increased where possible and tailor the output to the limits of the data. In this way, not only will a company's compliance analytics strategy exist at a topical level appropriate to that individual company, but it will also include the most complete and necessary data for those outputs.

Another common method to narrow the population is by deploying red-flag tests, which automatically flag anomalous or high-risk activity based on certain data attributes. These tests cannot be "copied and pasted" from one company to another; they must be tailored to the contours of the business in close consultation with cross-departmental stakeholders, such as internal audit, compliance, legal, and finance.

For example, one test is to flag transactions made to vendors not on a master vendor list. Before deploying this test, the company must first consider whether it is actually common practice to conduct business with vendors not on its master list, in which case the flag would be ineffective. Assuming this business does not commonly have transactions made to vendors not on a master vendor list, the company must understand if a lag exists between when a payment is made to a vendor and when the vendor is added to the master list. Finally, to probe even deeper, adding a vendor to a master data list likely involves screening the vendor, the efficacy of which could be another risk point in assessing a company's transactions. Data analytics lends well to this high degree of customization, making it easy to operationalize these tailored tests.

It's dynamic

In order for a compliance analytics program to be successful, it must address changes in business, regulations, world events, policies, and any other potential disruption. The DOJ highlights the necessity of compliance programs to be dynamic, saying, "One hallmark of an effective compliance program is its capacity to improve and evolve."[2] The memo continues to say that as business changes over time, "prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale."[3] Creating a dynamic compliance program with the capacity to adjust to changes relies heavily on data analytics.

Compliance analytics is not "set it and forget it." A critical part of the data analytics process is testing the model —evaluating the model output, incorporating feedback, and altering the model as the situation changes. When assessing that model, data analytics will review the results with a discerning eye, tuning the model to adjust for false positives, true negatives, and other findings. This iterative feedback loop is important for increasing the detection rate and reducing false positives.

Another aspect of the iterative feedback loop is periodically revisiting the model to adjust for any major changes to the business. For instance, the COVID-19 pandemic caused a precipitous drop in most companies' employee travel expenses. This meant that any analytics on travel and entertainment expenses had to be adjusted to account for the "new normal." Other consequential events include an acquisition, new regulations, or entering a new market. All of these could present new data sets and new risks to consider when tuning the model.

In addition to consequential events, observational data should also be considered when tweaking the model. For

example, new risks identified through auditing, monitoring, or other investigations should influence the risks considered with the compliance analytics model.

It delivers

While compliance analytics leverages technologically advanced methods, consumers should be able to easily understand the insights generated. A well-designed program will deliver actionable insights as opposed to an onslaught of difficult-to-decipher alerts and charts. The only thing worse than not employing compliance analytics is having a bribe sitting in a backlog or hidden in a complex graph.

When designed properly, data visualization dashboards are a great instrument to deliver compliance analytics. The goal of any compliance analytics program is to empower compliance professionals with the information they need to address risk at the company. Data visualization puts that information at their fingertips by providing access to the full data universe while pointing users to populations of interest.

For example, a well-designed vendor risk analysis module visualizes data from all vendors at a company while clearly illuminating the riskiest vendors of the pack based on the tests and risk ranking applied. The user should be able to interact with the visualization to filter data corresponding to the risky vendors, understand the various test results that are factored into the risk rating, and drill into associated payment transactions. In addition to specific vendor analysis, the user should also be able to filter views, dashboards, and analytics based on known business trends to easily identify the intersection of transactional risk and business strategy at large. In this way, the visualization provides compliance professionals with access to the details they need to determine if flags are false positives or require additional investigation and if they affect overall business strategy.

As with any new process at a company, user adoption and change management are critical to the success of a compliance analytics program. No matter how intuitive the visualization may seem, training and support are still necessary to help users acclimate to using the tool and ensure they are using it as intended. Engage the consumers in the design stages of the product to solicit their input on features and usability. Moreover, it is best practice to conduct user acceptance testing—or in other words, testing a new product to see if it stands up to the "real world"—prior to formally implementing the end product. The individuals at the company where the compliance analytics program is being implemented will ultimately be the program's users, able to identify insight and continue using the program after it has been fully created. They need to be able to understand the inputs to the program and make their own judgments to mitigate their company's risk and ensure compliance.

Implementation of a compliance analytics program requires thoughtful consideration and planning. However, it pays dividends: when used properly, compliance analytics helps companies better understand and manage their risks, identify risky behavior in real-time, and make informed decisions. Such dividends will mitigate the risk of compliance program inefficacy and will improve a company's insights into its own potential risk areas.

About the authors

Bridget Johnson is a forensic data analytics manager with over five years of experience applying data analytics to solve a range of complex legal and compliance problems.

Corey Dunbar specializes in data analytics pertaining to the detection of fraud, bribery, corruption, and compliance risks, and other forms of nefarious activity occurring within accounting, financial, and communicational data. Corey has experience working with large and small organizations at both their infancy or highest maturity in designing, developing, and implementing compliance monitoring solutions and platforms.

Morgan Dalton is a forensic data science specialist of BDO with over three years of professional experience in

advanced analytics for litigation matters and business intelligence.

Takeaways

- Proactively monitor your company's data, so that risky transactions and behavior can be detected prior to a potential violation.
- Capture data across disparate enterprise systems and business functions, structured and unstructured data sources, and third-party data sources.
- Tailor the program to the risks entailed with the business's industry, geographic footprint, and other unique qualities.
- Dynamically incorporate continuous feedback to tune and improve the data model and make it adaptable to changes in the business, regulatory landscape, and macro risk events.
- Deliver actionable insights on compliance gaps, potential risky behavior, or fraudulent activity in a manner digestible to compliance professionals.

1 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download.
2 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*.
3 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs.*