

MAX

Data defense

Protecting your brand



One of the most interesting themes in this year’s annual American Conference Institute’s event on the US Foreign Corrupt Practices Act (FCPA), held in Washington DC in November 2021, was the recurring emphasis on the use of data analytics in Anti-Bribery and Corruption (ABAC) compliance. The US regulators that aggressively oversee FCPA compliance, the US Department of Justice (DOJ), and the Securities and Exchange Commission and the monitors that are called upon to oversee enforcement of settlements and deferred/non-prosecution agreements, all reiterated an expectation that companies master the data in their organizations to enhance the use of data analytics in their FCPA compliance regimes.

For every company that has been in the position of making an FCPA-related disclosure to the US authorities, one of the critical pieces of their disclosure would have been around the nature, scope, and effectiveness of their ABAC compliance program. This is scrutinized by the authorities because the ability to demonstrate the comprehensiveness and effectiveness of a program factors directly into the calculation of any penalties, should the matter lead to enforcement action. Increasingly, the topic of data has been woven into that calculation because it is data that is critical to:

- 1) A company’ ability to effectively demonstrate the quality of its compliance program, and
- 2) The compliance team in their ability to monitor high risk activity and protect the company from unethical business activity in real time.

We explore below some insights into how data analytics and dashboarding can be used to harness the various streams of information that make up a compliance program, enhance the real-time functioning of ABAC risk monitoring, and drive efficiencies that mitigate the business impact of compliance prerogatives.

Why is analytics important to ensure FCPA compliance?


The best protection against an FCPA violation is an effective compliance program that goes beyond policies. Relying purely on compliance policies is not sufficient any longer, as organizations must now demonstrate to the authorities that they are leveraging data and analytics to gain insights and navigate risks. A technology-led strategy using data analytics and dashboarding is key in ensuring an effective and efficient FCPA compliance program. Companies need to actively monitor transactions to ensure compliance with policies. By identifying risk factors early and flagging anomalies, analytics and dashboarding can assist your compliance program with early detection, proactive alerting, and prevention. The trend now is to obtain a continuous view of FCPA risks rather than relying solely on a snapshot view. Analyzing data for trends and red flags keeps you in touch with the business and alerts you to changing risks.

Examples of how data analytics can be used:

A data analytics strategy can help assure compliance by looking for and identifying red flags, alerting on thresholds, setting parameters, and supporting the development of early warning systems. As the analytics matures, a company can look at powering a continuous monitoring system regarding key accounting controls as well.

A real-world example is in the field of business-to-business commerce. As organizations rely more heavily on channel partners to reach new markets and clients, indirect sales models are becoming more common. Furthermore, various levels of employees have the authority to approve higher pricing discounts and other non-pricing concessions to win new business, which raises operational and compliance risks significantly. For example, there are scenarios in which a partner sells at a deep discount to a reseller, who then uses the

large margin on that sale to pay a bribe to the end customer. Looking at discounting outliers from partner sales transactions may indicate a higher level of corruption that should be investigated in this case. Transaction size, region, typical discounting patterns, and other risk factors may reveal corruption red flags.

Data analytics can also be a very useful tool for companies to ensure that they are abiding by local laws, even in the case of rapid changes in guidelines. A salient example from the healthcare industry is summarized in Table 1. 

Data analytics can also be a very useful tool for companies to ensure that they are abiding by local laws

As countries such as the United Arab Emirates and the Kingdom of Saudi Arabia continue to witness major legal reforms, the Saudi Food and Drug Authority (SFDA) imposed new guidelines on pharmaceutical and medical companies to improve transparency of financial relationships among medical companies, healthcare providers (HCPs), and healthcare institutions (HCI). Failure to abide by such laws would lead to legal action against the company. As an example, medical companies must report all financial support provided to HCPs/HCIs exceeding SAR 500 per year to the SFDA. In addition, companies are only allowed to provide HCPs gifts in-kind for a modest value.

Based on our extensive experience in FCPA investigations in the Middle East region, we have identified several cases in which HCPs were:

- Paid above fair market value (FMV) for services provided;
- Provided financial support excessively across the year; and
- Provided excessive entertainment/ additional benefits.

Companies with a large volume of yearly transactions may find it challenging to track HCP/HCI spending per year or identify irregular transactions exceeding SFDA approved limits. Data analytics can strengthen the compliance program of the relevant companies by creating a dashboard which can identify red flags by analyzing the inputted data and policies as follows:

- Track financial support provided to HCPs/HCIs
- Notify the compliance team if the financial support provided to an HCP exceeds the approved limit by SFDA or the fair market value
- Flag any excessive benefits provided to HCPs such as business-class airline tickets or accommodation in 5-star resorts
- Flag any HCP sponsorships lacking a signed contract agreement between the relevant parties as well as the lack of notification of the HCP's employer

Another way analytics can aid in FCPA compliance is by creating a system of early warnings based on a set of internal control thresholds. The early warning system can detect unusual transactions that may be suspicious - it is these transactions and the companies' ability to prevent and detect them in real time where the proverbial rubber hits the road for FCPA compliance. Conducting automatic tests for gifts, entertainment, and charitable contributions, for example, can assist in identifying multiple gifts to a single individual or institution, or parties linked to a single institution. Analytics can also assist in identifying charitable contributions to government-affiliated organizations. The true strength of such a system is its ability to detect both discrete activities and suspicious trends.

Showcasing the compliance program itself

While it is critical a company's compliance team has the ability to actively monitor FCPA-related risks as they manifest in the business, it is also important for the team to have access to some slightly more "mundane" analytics as well. By this we mean corralling the various and often disparate ingredients of an FCPA compliance program itself into a single point of reference or dashboard. When the DOJ lawyers ask to see the evidence of a company's compliance program functioning, the company would be well served to demonstrate that it has ready and reliable access to the information required to make a positive assertion that its program is meeting the exacting standards set out in the DOJ's recently refreshed resource guide or the standards listed in ISO37001.

An FCPA compliance dashboard should be readily available to draw together the disparate components of a company's compliance program, which might include the following aspects (among others):

- The compilation and status of implementation of a body of robust, formalized policies (and associated

results of any effectiveness reviews completed of those policies),

- Evidence of a series of 'tone from the top' communications or the results of employee awareness polling,
- The codes of conduct and documentation or tabulation of employees' periodic acknowledgment of their responsibilities,
- Its whistle-blower program and the evidence of its use and nature/frequency of the channels and evidence of the company's efforts to respond, review, and tweak the channels for maximum effectiveness,
- Evidence of the online and in-person, localized, reinforcement training, and
- The compliance ratings/reviews of key individuals in high FCPA risk roles.

As with transaction monitoring, the effort required to harness this data into a central point of reference can be a deterrent to companies who might consider moving down this path.

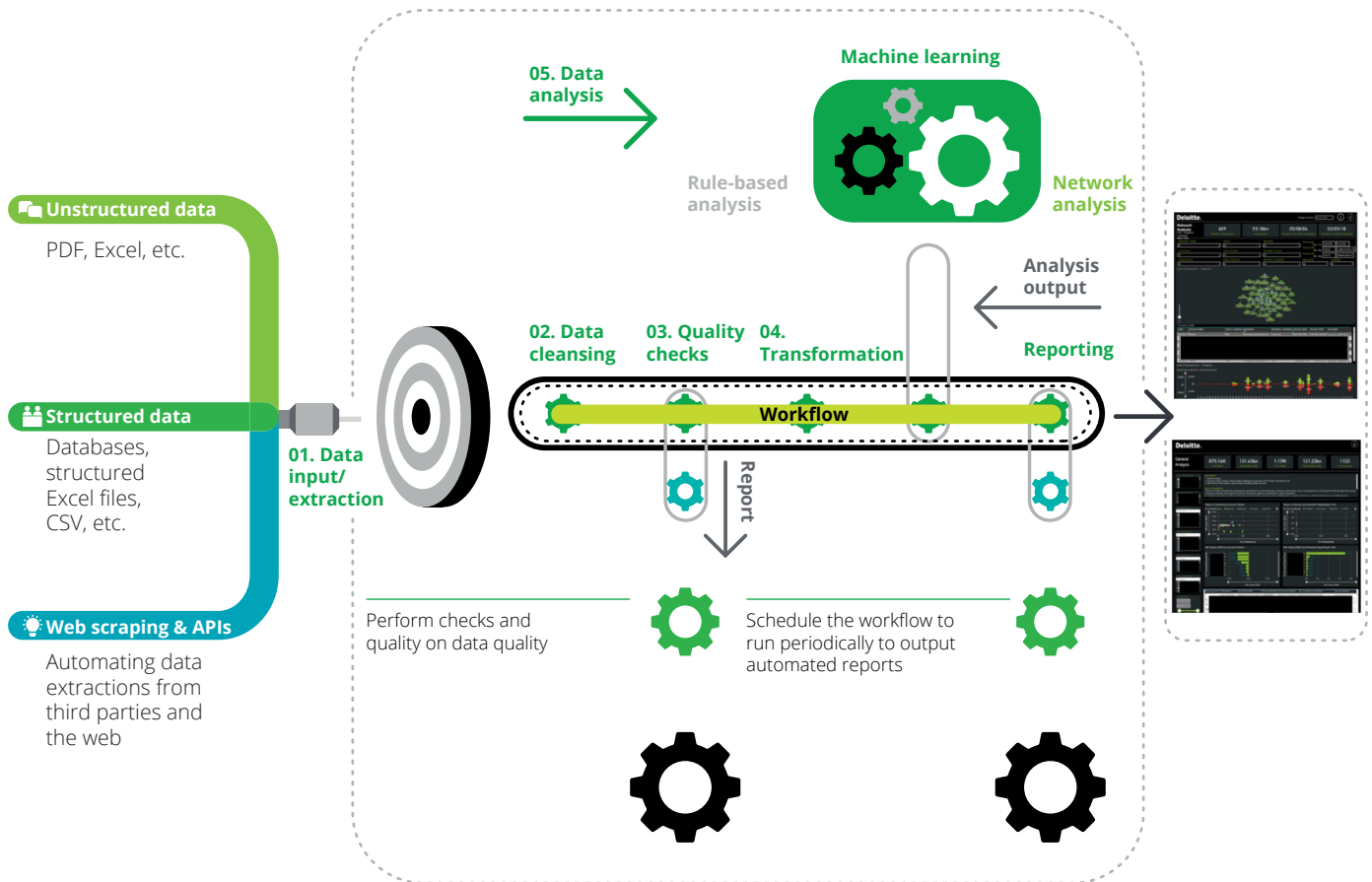
Setting up a compliance data infrastructure – a semantic graph addressing FCPA needs

Companies are frequently confronted with thousands of isolated data silos, posing an information overload challenge. Connecting datasets in a meaningful way, in our experience, is strategic for every business because it allows compliance leaders to gain context on an organization's transactions. Surprisingly, rather than a lack of information, the challenge for organizations attempting to automate compliance analytics is an abundance of information from disparate sources containing complex and vast amounts of data. A semantic graph allows a business to integrate and connect disparate data sets to not only unify and connect various sources of compliance data, but also to apply complex rules and patterns for automated compliance monitoring.

Three components are required for the effective design and implementation of an FCPA Semantic Graph:

- 1) Connecting disparate data silos
- 2) Examining interconnected data to uncover insightful compliance and FCPA patterns
- 3) Obtaining context-relevant knowledge from massive amounts of integrated data, for example, data from customer relationship management (CRM) systems, point of sale systems, and geographic and spatial systems

An FCPA compliance dashboard should be readily available to draw together the disparate components of a company's compliance program



For a company in the early stages of establishing their data infrastructure, this may seem like a massive undertaking. In reality, the initial steps would only consist of implementing a few properly deployed analytics to identify areas that require additional analysis, and the semantic graph would guide the processes going forward.

Looking forward, it is evident that data analytics will play an even greater part in ABAC compliance regimes from a preventive/detective perspective, as well as for a program quality monitoring perspective. Companies across industries will need to rapidly adapt and ensure their teams are able to access the required inputs, run various types of analytics, and

manipulate large data sets for different scenarios in an agile manner. This will best equip companies and offer protection against increasing regulatory scrutiny going forward. Therefore, establishing a sustainable data strategy and putting in place the infrastructure early on is a strategic move for all businesses, ultimately making the case for the effectiveness of the company's compliance programs and proving to regulators that you stand for action, not only promises. ●

By **Muzzi Ebrahim**, Partner, **Sridip Ganguli**, Partner, **Collin Keeney**, Partner, and **Wael Tahtah**, Assistant Director, Forensic, Deloitte Middle East