GIR
Global Investigations Review

JUST ANTI-CORRUPTION

How to build a data-driven compliance programme

10 December 2020

FRA's Neil Garodia and Weil Gotshal's Steven Tyrrell

The use of data and analytics continues to be an area of focus for both compliance departments and regulators in their assessment of the effectiveness of a corporate compliance programme. This theme continued in the latest iteration of the US Department of Justice's (DOJ) guidance for evaluating corporate compliance programmes released in June. Harnessing the power of available data to identify and mitigate risks is more important than ever. We explore what an effective data-driven compliance programme should look like under the new DOJ guidance, the challenges of implementing such a programme, and tips for overcoming these challenges.

First published on the *Global Investigations Review* website, 10 December 2020.

In day-to-day operations, companies of all sizes generate a massive amount of data from their systems. Many advanced compliance departments now use data analytics to improve detection of non-compliance and inform decisions about where to invest limited resources. Likewise, the US Department of Justice increasingly includes the appropriate use of data analytics as an important metric in evaluating compliance programmes. Overcoming the challenges of implementing a data-driven compliance programme is therefore a concern for all compliance departments.

DOJ's regulatory expectations are changing

Beginning last year, the DOJ began alerting companies in earnest that data analytics was a new focus for the agency. As former Deputy Assistant Attorney General Matthew Miner stated, the DOJ has leveraged data analytics in its own investigations to identify Medicare fraud, market manipulation, and other types of fraudulent activity. According to Miner, because "companies have better and more immediate access to their own data" than regulators, when misconduct does occur, "prosecutors are going to inquire about what the company has done to analyze or track its own data resources."

Further developing this theme, the DOJ revised its criteria for "Evaluation of Corporate Compliance Programs" in June 2020, providing new concrete guidance and emphasising the use of data analytics to enhance risk assessments and access to data resources, among others. This guidance has been further reinforced through the inclusion of certain key themes in recent deferred prosecution agreements (DPA), such as with Herbalife, Sargeant Marine and JPMorgan Chase.

Assuring compliance access to data resources

The revised DOJ guidance stresses the importance of compliance and control personnel having "sufficient direct or indirect access to relevant sources of [company] data" for the "timely and effective monitoring and/or testing of policies, controls and transactions." The DOJ also included this language nearly verbatim in the three DPAs mentioned above, further underscoring the importance of data access in compliance, no matter the size of the company. Herbalife and JPMorgan Chase are both multinational companies, while

Sergeant Marine is relatively small, and yet all three DPAs include the same obligations to create and facilitate data access for effective compliance monitoring. Elsewhere in the guidance, the DOJ also makes clear that companies should identify and address “impediments” to data access that exist in the organisation.

In practice, these items may require substantial changes in how companies provide internal access to key streams of information. Regulators may expect compliance and control personnel to work directly with the organisation’s accounting and information officers to identify important compliance-related data, so that it can be made freely available to control functions. Furthermore, regulators may expect companies to unify data and systems where there is not organisation-wide access due to previous mergers, acquisitions or other impediments.

Undertaking continuous risk assessment

The revised guidance also stresses that periodic risk assessments should be “based upon continuous access to operational data and information across functions,” and not be limited to a “snapshot” in time.

Incorporating this guidance may require a rethink of the process companies typically use to conduct risk assessments. Often, companies rely heavily on annual interviews and focus groups combined with review of periodic audit reports to identify risk areas that will be measured each year. This process necessarily creates an assessment that is limited to a fixed period of time.

The guidance suggests a more dynamic approach may be needed to supplement these efforts. By using data analytics to analyse patterns and trends, companies can identify real time changes that affect risk and then redirect assessment resources. Relevant findings can then be disseminated to management through real time alerts to make monitoring and spotting potential problems easier. For example, JPMorgan Chase received cooperation credit without a compliance monitor under its DPA for, among other things, increasing its electronic communications surveillance programme of trading activity and by “automatically ingesting and processing approximately 100 million messages” with a monthly review by analysts of “100% of the alerts generated from these surveillances.”

Testing, root cause analysis and remediation

The revised guidance carries over a previous recommendation that companies undertake continuous improvement by reviewing and auditing compliance programmes in the areas where there is known misconduct, including through the “collection and analysis of compliance data.” The DOJ has also incorporated this guidance into its recent DPAs, all of which require companies to use monitoring and testing of data relevant to prior misconduct to “conduct a thoughtful root cause analysis and timely and appropriately remediate to address the root causes.”

From this language, regulators expect that companies will use compliance systems to proactively identify areas of weakness and implement controls improvements before further misconduct can occur. The guidance also appears to encourage companies’ proactive efforts to make system improvements, rather than punish remedial action when systems later fall short.

The challenges for implementing a data-driven compliance programme

With the release of the new DOJ guidance, many organisations are realising it is now essential to update and modernise their compliance programme. Through our experience working in a variety of businesses and industries, we found there are some common challenges compliance programmes face on this journey to be more data-driven. Below, we point out these challenges and provide some tips on how to overcome them.

Lack of buy-in

Transforming a compliance programme to be data driven can be a long and arduous process that takes commitment by the organisation; getting buy-in and support from senior executives is essential. Without communicated commitment from the top, compliance groups have difficulty getting the process started for a variety of reasons, ranging from budgeting or resourcing to a lack of cooperation from the business itself. Experienced executives will have previously seen the outcomes for organisations who have not taken compliance risks such as corruption and fraud seriously. Therefore, communication at that level should focus on the most significant risks and their potential financial and reputational impact on the organisation. Additionally, quantifying the positive impact of implementing a data-driven monitoring approach and linking the impact to organisational KPIs and strategic goals will give further perspective to its importance. Finally, identify ways in which the data feeds, infrastructure, repositories, and analytics can bring added value to areas of the business with more direct linkages to the bottom line, such as operations and procurement.

No short-term strategic planning

One of the first questions a compliance programme will face in this journey is, "How do we start?" When this question is answered without specific near term goals, timelines, risk prioritisation, processes and/or outputs in mind, it leads to a lack of quantifiable progress and programmes that do not address key risks and incomplete projects. Begin small and targeted. The most important things to demonstrate when starting are progress and measureable value. This is best done with smaller, achievable projects. Think proof of concept. Furthermore, evaluate relevant factors in determining what risk area to focus on first. This process should include inputs like risk severity, availability of data, cooperation from the business and change management to ensure the objective can be met comfortably and the value can be demonstrated and quantified. Once the project is selected, ensure the execution team is representative of all relevant groups needed for successful completion (eg, IT, data governance, business experts, compliance).

Lack of data governance

In many organisations, especially larger ones, data resides in disparate locations, ownership is not assigned, access is difficult, and data quality can be poor. These are usually not issues that can be addressed overnight. That said, there are some steps that compliance teams can take to acquire reliable data in a timely fashion. As noted in the previous section, having a representative from the data and/or IT group on the transformation execution team is a must. They can help steer the IT landscape and facilitate identification of data gatekeepers. Additionally, focus on identifying the ultimate source of the data needed for the monitoring project. While this does not guarantee that it will be accurate, it does remove the layers of manipulation that introduce unintended risk. Finally, ensure the team understands the types of information in the data, so if sensitive data points are collected such as PII, risks and access are managed appropriately.

Ineffective operational model

Once the transformation has gained momentum through the successful execution of key monitoring projects, and there is a template for how to get these projects designed and implemented, the next step is to think bigger. Organisations that struggle to create value through analytics tend to develop analytics capabilities in isolation with solutions that are not scalable and without longer-term strategic goals. Think about data consolidation and access. Prioritise the datasets that are most valuable in mitigating key risks long term and consolidate them in a repository that is accessible to key risk mitigation groups. Ensure this is done within a technology infrastructure that is scalable, flexible to changing needs, and provides the proper security. The right resources, skillsets, and analytics capabilities are also necessary to best utilise the data and environment you are creating. Finally, align with the business where it makes sense. Where many compliance programmes start to lose traction is when they are seen as a hurdle to the progress of the business, rather than a partner in the journey.

Conclusion

Regulators will likely continue raising the bar regarding the use of data analytics as an element of an effective compliance programme. In response, successful companies will need to implement more data-driven compliance programs, reaping the dividends of increased efficiencies and improved risk management.

FRA's Dan Yeloff and Zandile Tshuma and Weil's Carl Duffield and Cecile Casali also contributed to this article.

First published on the *Global Investigations Review* website, 10 December 2020.