strategy+business
a pwc publication

Tech & innovation / Spring 2021/Issue 102

Meet modern compliance: Using AI and data to manage business risk better

The combination of data analytics and artificial intelligence can give organizations a competitive advantage and mitigate risk along the value chain.

by Kim David Greenwood, Sean Torcasi, and Matt Kral October 22, 2020

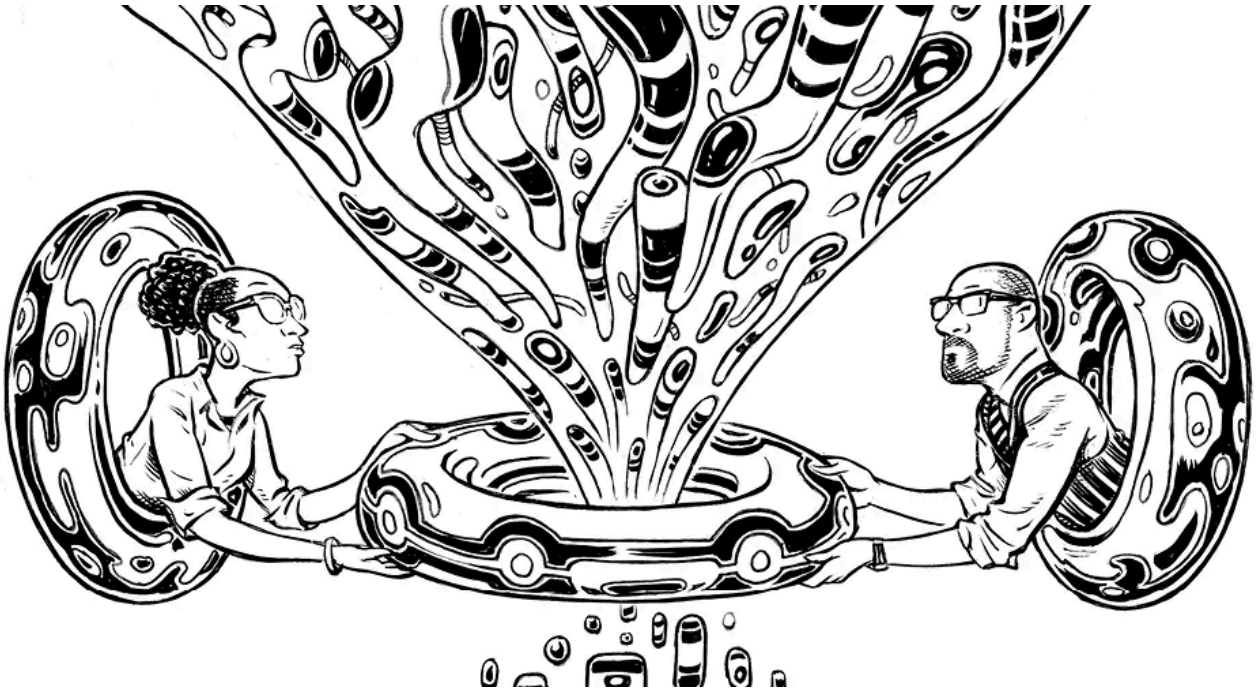

Illustration by Lars Leetaru

A version of this article appeared in the Spring 2021 issue of strategy+business.

In June 2020, when the U.S. Department of Justice (DoJ) issued updated guidance on how to evaluate corporate compliance programs, it came with a clear mandate to companies: Compliance programs must use robust technology and data analytics to assess their own actions and those of any third parties they do business with, from the point of engagement onward. At the very least, companies are expected to be able to explain the rationale for using third parties, whether they have relationships with foreign officials, and any potential risks to their reputation.

This is a compliance game-changer. Historically, organizations could argue that they simply did not have the information available to identify potential compliance dissonance across their networks: the "needle in a haystack" defense. Organizations are now expected to show that they are leveraging data and applying modern analytics to draw insights and navigate the risks across their *entire* business network.

Many companies, including large multinationals in a variety of sectors, have not focused on this area, because they have regarded compliance simply as an obligation or even an afterthought. They are missing an opportunity. Using the modern tools available today to ensure strong third-party risk management and even internal risk management can lead to better deal or contract hygiene and bolster data protection; it can also help craft environmental policies and evaluate health and safety risks, including in cybersecurity, which is particularly important as the COVID-19 pandemic has created a rise in remote working.

The DoJ's updated guidance is clearly intended to enhance the detection of any fraud or corruption. This includes determining whether compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies and controls. In turn, this has put a spotlight on how organizations are investing in technology to support these areas.

Third-party management, powered by technology, is now a baseline expectation of the DoJ in any of the prosecutions it brings under the Foreign Corrupt Practices Act (FCPA), the U.S. legislation that allows for the prosecution of corruption and fraud perpetrated outside the United States, by both U.S. and non-U.S. businesses (and the people associated with them) that have any business operation in the country. "The recent guidance is a big deal to someone like me who is focused on the continuous improvement of our compliance program," said Alan Gibson, an assistant general counsel in Microsoft's office of legal compliance. "The emphasis on data analytics and third-party risk management has evolved to the point where we are no longer just reading between the lines. The expectation that companies use these tools has been expressly called out."

The long arm of the law

The impetus for change has been building. Business is getting inherently riskier owing to global operations and increased reliance on third parties. Meanwhile, technology is helping bodies like the Securities and Exchange Commission and the DoJ get smarter about uncovering wrongdoing. (The U.K. Bribery Act and other European laws are also targeting corruption around the world.)

Consider the numbers: In the past decade, there has been a significant increase in prosecutions and fines both in the U.S. and elsewhere levied against companies for corruption. Fines imposed for FCPA violations, for example, have increased exponentially. The average fine in 2010 was a few million dollars; in 2019, it was US$135 million — out of a total of more than $2.5 billion levied in sanctions, according to research by Stanford Law School in collaboration with law firm Sullivan and Cromwell. The single biggest fine this year was nearly $4 billion.

The range of penalties for compliance failures is wide, as demonstrated above. From a fine of less than $2 million for substandard record-keeping, for example, the penalty can quickly climb. And a lack of data to support predictive capabilities is no longer an excuse that the DoJ is willing to accept. “We want companies to invest in robust and effective compliance programs in advance of misconduct, as well as in prompt remedial response to any misconduct that is discovered,” said then DoJ deputy assistant attorney general Matthew S. Miner in a September 2019 speech at the Sixth Annual Government Enforcement Institute in Houston. As a result, the current and likely future guidance on third-party compliance reflects the authorities’ new appreciation for what the technology can do.

Turning sticks into carrots

Microsoft has been part of pioneering efforts to develop tech-enabled solutions that can address regulatory requirements and more broadly combat corruption. These efforts demonstrated the power of digital tools to proactively identify, predict, and monitor bad behavior and bad actors. But companies should not see these modern compliance requirements only as a stick. Advanced technology that is predictive and proactive, and that results in better visibility into the risk landscape, offers more than protection from investigations and prosecutions. For businesses that want to thrive in today’s data-driven environment, such technology provides a technological competitive edge: table stakes that can both mitigate risk and help greenlight opportunities with more confidence because the risks have been properly evaluated.

Strong, tech-enabled, third-party risk management capabilities can strengthen corporate governance, which will in turn enhance reputation and build trust. In essence, compliance should no longer be seen simply as a backroom cost center. Rather, it is a means of strengthening the

business brand, increasing productivity, and driving growth of market share, with relevance at the C suite and at the board level.

According to Marko Kuzmanovic, the Microsoft finance director who oversees planning, growth, and innovation for Microsoft's high-risk deals desk, "By engaging early in the sales contract life cycle and providing compliance oversight and ongoing risk education, we [at Microsoft] have been able to realize better, more compliant deal construction. This is critical at quarter-end when deal volumes spike. Sellers internalize the risk guidance and proactively ensure their contract meets the company's compliance standards — often reducing monetary concessions that improve margin and profitability."

Bring tech to the party

Four years ago, PwC and Microsoft worked closely together to further develop a tech-enabled compliance analytics suite of tools called Risk Command. "We started the journey to respond to internal and external pressures to embrace a 'data-driven' approach," Gibson recalled. "But it appears to be what regulators are now expecting and serves as a benchmark for what others may want to do."

These compliance analytics tools have expanded from an initial due diligence aid to form solutions that combine and consider multiple risk factors or attributes. They include where businesses operate, odd patterns in transactions, atypical discount levels, unusual sales velocity, or other details that might suggest an increased level of risk or out-of-the-ordinary activity. The tools are powered by a machine learning model that analyzes the attributes of each potential risk — be it a contract or a potential partner, for example — from a wide variety of public sources and in-house data, and feeds them into an algorithm that gives them a risk score on a scale of 0 to 100. This analysis, strengthened by the size of the data lake — the collection of available data — provides insights into both third parties and related sales transactions. And, with each use, these predictive analytics get smarter and more adept at identifying anomalies, effectively building a better mousetrap to prevent noncompliance.

The system monitors activity in real time around the world, 24/7. But it is still the case that people need to review the insights and provide a human evaluation to mitigate compliance risks. This is job one. Getting the full value from investment in the technology comes when the insights it produces can be used to develop a more strategic approach to compliance, which could be called a compliance-by-design operating model.

In a sales contract, for example, data comes from a variety of sources that need to be structured and input into the system. The real magic happens when that data leads to insight. "This is not just about providing visualizations or reporting," explained Microsoft's Gibson. "This goes beyond simply

providing business intelligence, because it tells you what's risky, why it's risky, and how to effectively mitigate that risk. That's the special sauce that allows us to go from data to insight to action."

The flexibility of technology like this lends itself to a wide range of compliance applications, from mitigating corruption risks, to cybersecurity and privacy issues, to antitrust, trade, intellectual property, and litigation. This is where compliance departments can create a competitive edge. As an example, to ensure sales contracts have appropriate intellectual property (IP) protection, the system might be set to flag expiring patents, search for any potential IP infringements, highlight anomalies in manufacturing or in the supply chain, and provide automated contract review. It could also be set to identify and mitigate cyber-threats before they infect their network, with automated data privacy reviews on digital assets.

Better command and control

Pharmaceutical companies have long been prone to governance concerns, which has led to many facing significant fines for poor risk management in such areas as drug testing, trials, and marketing. In some instances, companies have been caught bribing doctors to prescribe medicines or producing misinformation, intentionally or not. Beyond the supply chain and the quality and safety of its products — otherwise known as pharmacovigilance — key risk areas include privacy and promotional practices. These multilayered and complex activities are ripe for abuse, putting companies in the sector under the regulatory microscope, which often results in fines and costly legal action.

"

This goes beyond simply providing business intelligence, because it tells you what's risky, why it's risky, and how to effectively mitigate that risk. That's the special sauce."

For one global pharma giant, PwC helped build a risk control system that used a large number of external and internal data sources to flag the highest-risk third parties that required additional due diligence before contracting. In a three-month period, it flagged more than 50 potential risks that the company was able to address before any of them materialized into an issue.

Whatever the size of the business, one of the challenges of using a system that leverages AI or machine learning is building trust among internal stakeholders. False positives and false negatives can occur with machines, just as they can with manual research. People need to know the mousetrap is going to catch the mouse. Pilot programs, running historical data on deals known to have been problematic, can help demonstrate that the AI would have identified the issue in real time.

Most compliance lawyers know about blockchain and bots, so it's not a leap to show how this technology can be applied to internal compliance processes. For example, a multinational industrial manufacturer recently began a pilot using Risk Command to conduct real-time contract reviews in which analytics could scan documents for potential problems relating to payments to third parties. Although the manufacturer can operate in many high-risk markets where U.S. companies cannot, such as Iran, doing so may jeopardize its U.S. business; this being the case, the procurement team needs to have information that ensures it does not make payments to blacklisted firms. The dashboard is programmed to give them a heads-up so they can take preventive action.

When two large carmakers merged, for example, and needed to vet the combined global network of dealers and third-party suppliers, PwC worked with them to build a risk management technology solution that standardizes and customizes the onboarding process and performs due diligence. The tool can mine data from the internet to detect, for instance, whether a supplier has been put on a "do not engage" list or is the subject of any allegations of corruption.

Underestimating strategic risk is one of the top causes of shareholder value destruction, but basing risk and compliance decisions on machine learning can dramatically impact all areas, from sales and marketing to finance. It can lead to higher-quality deals for the sales force with fewer discounts. It can lead to higher levels of service and better partner satisfaction. It can build trust through the whole value chain. The new importance that prosecuting authorities are giving to robust compliance data analytics will likely spur investment in these technologies, but the message is that they are not simply a defense. They can be an integral part of strategic decision-making.

"The analytics can help you to assess and manage the risk, but the hardest part isn't gathering the data — it's taking the action," said Gibson. "The partnership with the rest of the business is the key to pulling this off." With the authorities now explicitly expecting companies to gather the data and use analytics, those that are first movers in this space will enjoy significant advantages.

Author profiles:

Kim David Greenwood specializes in transformation, growth and innovation, and risk management strategies for Strategy&, PwC's strategy consulting business. Based in San Francisco, he is a principal with PwC US.

Sean Torcasi focuses on internal audit, compliance, and risk management services in the technology, consumer markets, and health sectors. Based in Seattle, he is a partner at PwC US.

Matt Kral helps organizations set the vision, governance, and operating model for compliance programs, focusing on using technology to mitigate risk. Based in Seattle, he is a director with PwC US.

Also contributing to this article were Natasha Ellis, Michael Green, and Mitchael Houtsager of PwC US.

Topics:

compliance | data analytics | decision making | ethics | risk | risk management