BMA ADVOGADOS

Compliance in a 100% digital environment: how to mitigate the risk of increased fraud in new corporate processes

06.05.2021 3 min read

Authors

Anna Carolina Malta Spilborghs

Related areas

Compliance, Investigations and Regulatory Enforcement

Topics

Compliance, Investigations and Regulatory Enforcement

Compliance ESG COVID-19 Anna Carolina Malta Spilborghs

Changes in working environments that had been the subject of debate and discussion, and were expected to take place over a period of five to ten years, occurred almost overnight.

Since March 2020, when the covid-19 pandemic was declared, businesses from various sectors, some with little or no experience in remote work, have had to adapt their work environments to social isolation measures.

Many companies found themselves compelled by necessity to adopt telework, which, for 51% of Brazilian companies, was entirely new. Changes in working environments that had been the subject of debate and discussion, and were expected to take place over a period of five to ten years, occurred almost overnight.

But how did corporations react to these sudden changes?

2020 was a year of adaptation. Now, in 2021, organizations have more experience with remote work and have managed to create working conditions designed to mitigate the opportunity for fraud. To do so, however, they have had to invest in training, improvements in processes, and monitoring of their workforce and their various stakeholders.

In a time of growing cybernetic fraud, one of the most important challenges for businesses has been to provide their teams with access to systems so that they could do their work remotely, in order to maintain the business's essential operations, while at the same time ensuring efficiency, security and protection of data.

But investing in strong systems is not enough if a company's workforce is not prepared, since it is an organization's people who are the first line of defence. Collaborators of all types, not just employees, should have access to permanent training on matters ranging from techniques for preventing and defending against e-mail attacks, to behavioral risks and standards of conduct: they need to be aware that what they do is essential to the company's security.

Many studies of fraud point to a business's suppliers and other commercial partners as the weak spot in its compliance practices. In turbulent times such as these, it is essential for businesses to reinforce their background checks, review their contracts, and analyze the financial situation of their commercial partners and potential new suppliers.

There has been much talk about the power of new technologies, and especially artificial intelligence and machine learning, in the detection of frauds and cybernetic attacks. Although they require significant investment, businesses that had begun adopting these new technologies prior to the pandemic entered the crisis from a position of greater strength, with better capacity to monitor their systems, identify potential failures, and repel cyberattacks. But many other companies quickly realized the importance of fraud detection and cybersecurity and implemented their own programs or hired specialists to help.

The main point is that compliance monitoring must evolve with the times, so that businesses can identify problems as they arise, take steps to mitigate those problems, and anticipate future developments.

**This content is part of the e-book "A Post-Covid World, the ESG Agenda and Other Trends in 2021: Insights for Foreign Investors in Brazil". Click here to view all the articles.*

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Anna Carolina Malta Spilborghs