Poorly implemented tech leads to enforcement investigations at 40% of global companies - report

A landmark survey of more than 1,500 compliance leaders around the world, including in Africa, has revealed major risks associated with digitalisation, with 41% of those surveyed admitting their organisation has already experienced enforcement investigations by regulators because of technology that was poorly on-boarded and/or implemented. According to this new research *The Currency of Connection: Mobilizing Technology for Compliance Integration*, investigations are most likely to arise in relation to data privacy and cybersecurity, as well as tax, transfer pricing, fraud and antitrust.

© alphaspirit – 123RF.com

Janet MacKenzie, Partner and Head of the Technology, Media and Communications Industry Group at Baker McKenzie in Johannesburg, explains that only 26% of African respondents in this survey (compliance leaders based in Cote d'Ivoire, Egypt, Ethiopia, Ghana, Kenya and South Africa), had been subject to a compliance investigation as a result of poorly implemented business technology.

Legislation challenges

Mackenzie explains that this lower percentage of investigations in Africa is mostly due to the widespread lack of legislation covering the technology sector in Africa - numerous countries in Africa do not yet have specific legislation around cybersecurity, and data privacy and protection. In countries where regulations do exist, the laws can be vaguely worded, and there are challenges around enforcement.

"Regionally, for example, the Southern African Development Community and the Economic Community of West African States have data protection policies in place, and the African Union's Convention of the African Union (AU) on Cybersecurity and Personal Data (2014) has been ratified by seven countries so far, but it needs the ratification of 15 member states to become effective.

“Legislation governing the digital economy is essential to protect African citizens in terms of both their digital privacy rights and cybersecurity threats, while at the same time also ensuring that their online freedoms are not threatened. The AU has been encouraging its member states to sign the agreement and implement balanced local legislation that is fully enforceable and that respects human rights.

“To facilitate this process, consultations with stakeholders in government, businesses (local and international) and organisations representing wider society, would ensure a balanced approach during the drafting of these laws. International legislation has to be considered alongside local laws, given the borderless nature of the online environment, and consulting with technology experts on policy means that due consideration can be given to the specific nature of this rapidly developing sector. Considering the current rapid move to digitally focused business models in Africa, the implementation of these legal protections and guidance has become urgent,” Mackenzie notes.

Guidance gaps

Gaps in legislation is an issue for regulators in other jurisdictions as well, who, in some cases, are continuing to play catch up. Some 53% of the 1500 compliance leaders surveyed report that a lack of consistent guidance on compliance technology from regulators globally is a barrier to further tech adoption. Most respondents expect this to change, with almost two thirds (64%) of compliance leaders predicting that scrutiny of tech-enabled business models and data privacy issues will now be top of their regulators' 'to-do lists'.

The research also reveals that compliance teams, who are often a key line of defence against such enforcement investigations, are largely shut out of decision making around new tech, including a third of businesses surveyed who believe their organisation is employing new technology without any regard for potential compliance and regulatory risk at all. 34% of African respondents said that the compliance function had no oversight of new technology and that they were not consulted on purchase decisions.

4 tips to starting a compliance function

Ezra Pillay 18 Nov 2020

To drive their own efficiencies, manage cost pressures (56% of compliance leaders have seen their budgets cut due to Covid-19) and to keep up with the digitalisation of their wider organisations, compliance teams themselves are therefore also increasingly turning to tech. While this has largely to date been focused on relieving the administrative burden, most compliance teams are on the cusp of more ambitious investments.

According to Joanna Ludlam, Global Co-chair, Global Compliance & Investigations, Baker McKenzie: "Within the next two years, the overwhelming majority of compliance leaders plan to further adopt machine learning, AI and predictive analytics within the function, and we are already seeing some advanced use of digital tools among tech-enabled compliance teams — including bots for finding and delivering information as part of compliance training and data-backed systems designed to identify concerning patterns of behavior."

However, maximizing the value of compliance technology is still challenging for many. Only 56% of compliance leaders report that compliance technology is effectively achieving its primary purpose, while 63% agree there is value yet to be realized from their digital tools. In Africa, 54% of believed that the value of these digital tools would be realised in future years.

The third party challenge

One area where there is increasing concern and scrutiny is related to third party compliance risk, and in particular where a company has a minority interest, a JV, or regarding supplier relationships.

Technology is therefore being rolled out to support compliance teams implement best practice and manage risk among investment partners. According to our research, 45% of compliance leaders plan to deploy technology to monitor the actions and behaviors of these third parties.

Tristan Grimmer, Compliance and Investigations and International Trade Partner, said: "We are seeing a rise in the use of risk assessment tools to conduct pre-partnership due diligence as well as oversight on an ongoing basis — streamlining the process of capturing and maintaining information that enables the identification and assessment of compliance risks. This trend is likely to accelerate as new technology comes to market."

Artificial intelligence (AI) is particularly useful in managing third party risk. It can mine, collate and analyse public source information relating to investment partners to make connections that otherwise may not be made and highlight risks that may otherwise remain hidden. Used in this way, AI can provide greater insight and transparency on investment and procurement decision-making, thereby making it easier to assess potential hotspots.