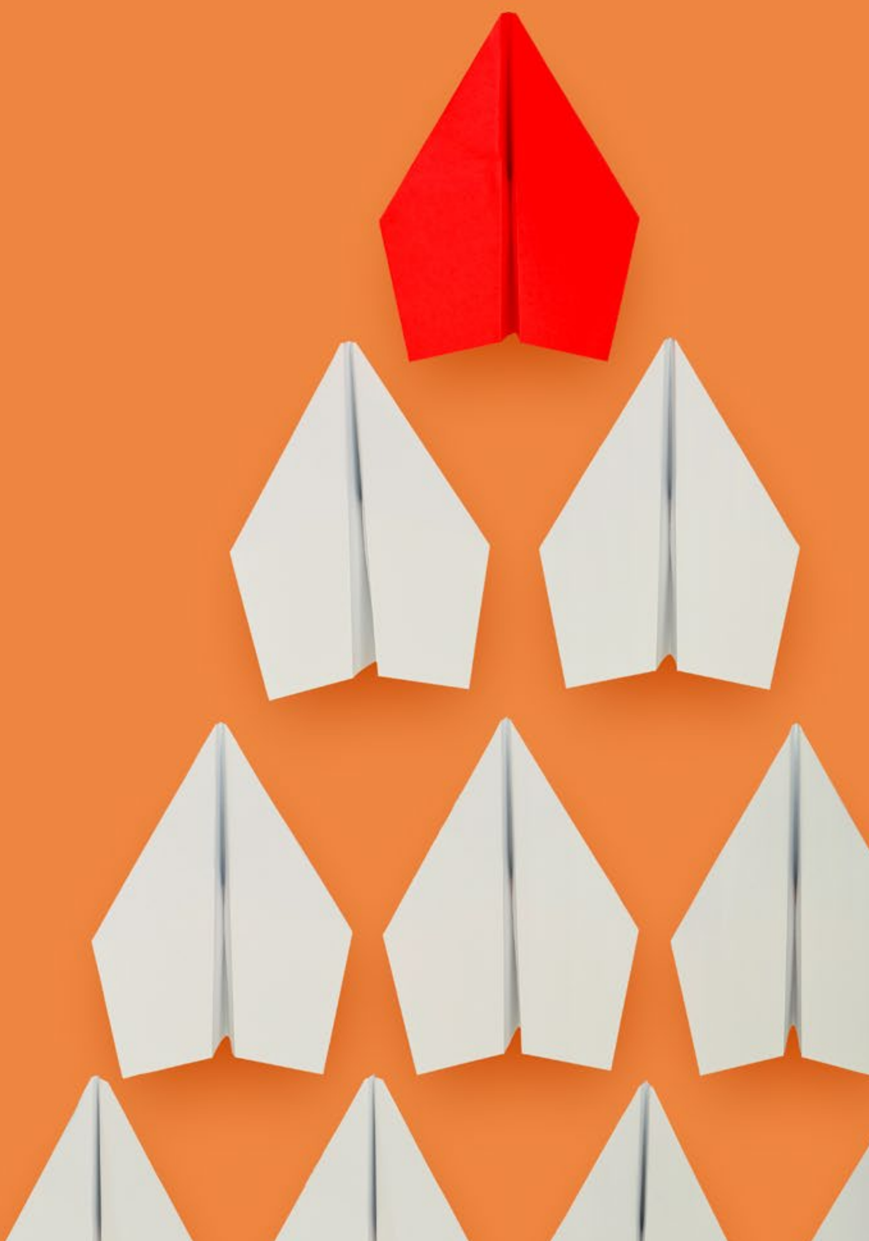
Audit Committee News
Edition 55 / Q4 2016 / Risk Management & Compliance

The future of Compliance



The challenges facing compliance officers appear to grow year by year. Compliance in the non-financial sector is not anymore "THE" hot topic for Anglo Saxon corporations, but also a reality for European and Swiss corporations, given the huge rise in the number and complexity of regulations, more rigorous enforcement by authorities, and, as important (if not more), societal expectations on corporate ethical behaviors. Compliance officers are expected to more effectively prevent compliance incidents from happening but… the reality is that no sooner is one risk dealt with, than another arises. This is the product of today's fast-moving, globally connected world.

From a central /control oriented function, with an image (and sometimes role) of a corporate police, confined to regulatory and legal compliance, the role of compliance is now expanding as it becomes generally better understood, incorporating a flexible definition that also covers ethical standards, sustainability and much more. But the evolution of the function also entails other components:

The cost of compliance

Compliance is an expensive function, hence focus has to be given on the value that the compliance function delivers and which structure provides the corporation with the best competitive advantage… It is about optimizing the internal compliance model and making best use of investments, which can involve decisions such as shifting a highly centralized, heavily staffed model to a more decentralized or hybrid model.

The transformation of the compliance role: from highly centralized, to a hybrid or even decentralized system

There is a current perception that compliance functions are by definition large administrative functions, involving a high number of compliance officers. This perception is largely inspired by the banking compliance model, where compliance officers often also play a role of internal controllers. But in essence, as highlighted by a recent publication from economiesuisse, there is no one size fits all.

There are mainly three compliance organization models:

- Centralized; the compliance function retains direct control over all compliance-related activities and execution of controls. A common structure in highly regulated sectors such as the financial services. It often involves a large team of dedicated compliance officers
- Decentralized: Compliance is embedded in existing functions (finance / human resources etc). Compliance activities are carried out by function, with limited central oversight
- Hybrid: Responsibilities for compliance activities are delegated within the organization, but the oversight and ultimate responsibility are borne centrally or regionally (if the corporation is a large multinational).

Whilst a fully centralized structure can be perceived as "safer" from a compliance risk prevention (especially when the industry is highly regulated) as it includes a strong controlling role, this model is falling out of favor. The cost of funning such a function, but also the perception that compliance is the responsibility of a single department rather than the whole organization are the key challenges associated with those structures. By contrast, a hybrid or decentralized compliance structure will have to embed compliance culture and controls across the various parts of the business, moving the role of compliance officers from a controlling role to a more strategic/advisory role, which will monitor regulations and use data analytics to drive the design and execution of compliance programs at an operational level.

The transition from a centralized to a decentralized or hybrid model must be driven very carefully, in order to maintain the effectiveness of compliance controls and the compliance culture. Regular communication, training and the setup of a dedicated compliance control framework are key elements of an effective compliance function, even in a decentralized model.

The role of technology

Throughout these changes, technology – and in particular data analytics tools – will play an increasing role in managing compliance programs. More accurate insights, delivered faster and earlier through a focused compliance dashboard are essential to prevent compliance breaches and give the corporations the metrics to demonstrate (or not) the effectiveness of their programs. This also supports a decentralization of the function, by which each department is an actor of compliance.

The risk associated with third parties

A shockingly high proportion of businesses fail to formally identify high-risk third parties when, in the meantime, companies typically deal with a multitude of business partners such as vendors, distributors, sales agents etc. The result can be serious exposure to potential compliance risks, not to mention possible infringement of laws such as the UK Bribery Act and the US Foreign Corrupt Practices Act.

In parallel, authorities and the public expect high standards of integrity not only from the corporations themselves, but also from the third parties dealing with those corporations. In Switzerland, inspired by the UK "Modern Slavery Act", the upcoming Swiss initiative called "The Responsible Business Initiative" goes in that same direction: "Companies will be legally obliged to incorporate the protection of human rights and the environment in all their business activities. This mandatory due diligence will also be applied to Swiss based companies' activities abroad."

The duty of the board of directors

In Switzerland, art 102 of the Swiss Criminal Code states that if a felony is committed in a corporation, and if it is not possible to attribute this act to any specific natural person due to an inadequate organization, then the felony is attributed to the corporation – in which case such

corporation is liable to a fine not exceeding CHF 5 million – the following case is a perfect illustration of this: A company had to pay a fine of CHF 2.5 million and a compensation of CHF 36 million for violating these provisions in a bribery case, as the prosecutor stated that "the company had failed to take necessary and reasonable organizational measures to prevent bribery of foreign public officials". In other words, boards are not exempt of compliance responsibilities and must ensure that the right compliance management system is in place so that compliance operates effectively within the corporation and that any breaches of laws or standards are identified and dealt with swiftly.

The threats from inside

Highlighted by the recent cases experienced by large banks, it is now understood that employees and trusted business partners are the main cause for compliance breaches. Understanding and isolating this risk is difficult given their access to a corporation's systems and premises, but technology can help mitigate the risk.

Despite what one can hear or read, "Compliance" is not the new flavor of the day which is due to be out of fashion in a couple of years. Regulators in Switzerland and globally tend to impose more regulation on corporations, and higher governance requirements. Enforcement accompanies those regulations, and infringement to those compliance regulations can have massive effects not only financially but also on the entity's reputation.

In conclusion, a well-managed compliance management system becomes slowly but surely a "must have" function for all corporations with international exposure, to protect their business and employees from the high reputational and legal risks related to non-compliance, and to provide a basis for sustainable growth. However, in order to ensure that this function does not develop into a paper tiger, a great level of attention should be dedicated to designing a compliance management system that effectively meets the corporation's needs, risks and culture.

Solveig Rufenacht
Head of Compliance, KPMG AG
srufenacht@kpmg.com