Risk & Compliance Management

Contributing editor
Daniel Lucien Bühr

2017

© Law Business Research 2017
Global overview

Daniel Lucien Bühr
Lalive

This first edition of Risk & Compliance Management in the Getting the Deal Through series reflects the growing awareness in private and public organisations that they should know their legal risks and handle them appropriately. Legal risks are among the most important hazards organisations face. Consequently, diligent legal risk management is essential and senior management should have a genuine interest in effective legal risk management because risks that materialise may severely impair not only their organisations but also, at a personal level, their career prospects.

Risk, as defined in ISO Standard 31000, is the effect of uncertainty on objectives (ISO Standard 31000 – Risk management, section 2). That effect, which is a deviation from the expected, can be positive or negative. Therefore, risk always includes opportunity. Of course, no real business opportunity exists without risk. Tolerating risk would therefore not be such a bad thing, were there not the flipside of the coin in the form of negative impact on objectives. The negative effects of legal risks on objectives can wipe out companies overnight, regardless of how powerful they are.

Effective legal risk management should therefore remain at the top of board agendas. Judging from the uninterrupted stream of criminal and administrative investigations and sanctions against businesses across the globe, it would appear that legal risk management is either not on board agendas or that, although they may focus on legal risks, boards are ineffective in managing them.

The costs associated with failure to prevent non-compliance with the law are astronomical. Interestingly, or perhaps logically, corporate expenditure on risk and compliance management is either nil (companies that do not yet have any risk and compliance management) or almost nil (most companies with a compliance function spend only between 0.01 and 0.3 per cent of turnover on compliance, i.e., some where between US$500 and US$3,000 per US $1 million turnover). A look at those companies that do manage risk and compliance, however, reveals that many are (still) struggling with the effectiveness of the systems they have introduced.

The most accepted explanation in the risk and compliance community is that resources are mostly spent on irrelevant exercises, such as screening public records for sanctioned persons (who, in all likelihood, would not be acting under their own name but through intermediaries or legal structures) or conducting e-learning with employees who may be using lists with the right answers to speed up what they see as a time-consuming process.

And what about the most powerful drivers of organisational integrity and compliance: leadership, values, remuneration and culture? These do not generally appear on compliance budgets at all. It is estimated that, at best, only 1 per cent of compliance budgets is spent on the key drivers of organisational integrity and compliance. So this is one possible explanation for the ineffectiveness of today’s legal risk management.

Interestingly, a number of businesses, including global players, are now investing heavily in fintech software to monitor employees and identify legal risks. It remains to be seen how effective this is, particularly in businesses where executive board members in the past and maybe still today agreed to not communicate by e-mail. Judging from the compliance learnings of the past 10 years, it would appear that the employment of monitoring technology is embedded in a robust policy built on leadership, values and a culture. If this is not the case, the employment of monitoring technology is likely to generate costs – although at best it will create few results and at worst create new, maybe even greater legal risks (one important aspect of the legal risk treatment process is assessing whether modifying risks, i.e., mitigating them, leads to new risks).

According to the media, Ravi Menon, the managing director of the Monetary Authority of Singapore, expressed a similar view at the Australian Securities and Investments Commission Annual Forum in Sydney on 20 March 2017. Mr Menon said that robo-advisors, an increasingly popular form of fintech wealth management software, can help reduce money laundering risks, yet could increase systemic risks by causing investors to suddenly rush for the door all at once. Robots, our new friends, will help us manage certain risks but will, as stated by Mr Menon, also create new ones - maybe bigger ones than we can imagine today.

Another important new aspect of risk management is regulatory technology, or ‘regtech’ – also known as supervisory technology or ‘suptech’ – such as compliance software used by banks. This will play an important role in in-house risk and compliance management and regulatory surveillance. It will be of the utmost importance for users to remain intellectually ahead of such software if they are to fully understand what results it can deliver and what new systemic risks will inevitably arise. It is worth stating once again that technology will never be a substitute for leadership, values, culture and good governance.

In the recent past, two developments have been setting a global trend in organisational risk and compliance management:
• the international standardisation initiatives by organisations such as the International Organization for Standardization (ISO), the Committee of Sponsoring Organizations of the Treadway Commission (COSO) or the Basel Committee on Banking Supervision (BCBS); and
• multilateral or unilateral government guidance provided by, for example, the Organization for Economic Cooperation & Development (OECD) and the US Department of Justice (DOJ).

Recent key initiatives are the release of:
• ISO Standard 19600 - Compliance management systems;
• ISO Standard 31001 - Anti-bribery management systems;
• updated ISO Standard 31000 - Risk management;
• the updated COSO ERM(Enterprise Risk Management) framework;
• the BCBS Standards and Guidelines on governance, risk and compliance management in the banking industry, for instance:
  • BCBS 239 - Principles for effective risk data aggregation and risk reporting;
  • the G20/OECD Principles of Corporate Governance;
  • the DOJ Compliance Initiative; and
• the Criminal Division Fraud Section’s March 2017 topics and sample questions for the evaluation of a corporate compliance programmes.

All these standards and guidelines have common denominators: leadership; culture and systematic governance, risk and compliance management. The main lesson to be learned from the governance, risk management and compliance breakdowns of the financial crisis is that the prerequisites for successful and sustainable business are good, accountable leadership; the promotion of a culture of