Compliance management

Daniel Lucien Bühr
LALIVE

Compliance management systems: A quantum leap for the revival of corporate leadership, values and culture

Businesses implement compliance programmes to ensure they comply sustainably and effectively with the law. Given numerous fines imposed recently on leading businesses around the globe for repeated, 'systematic' infringements of the law, it can be inferred that compliance programmes in general fail to keep their promise.

Assuming that, on the whole, corporate compliance programmes are indeed less effective than they should be (evidence to the contrary is, of course, always welcome), the question immediately arises about whether there is a cure. One of the most prominent developments over the past few years has been the introduction of compliance management systems.

A compliance management system is an integrated process based on strategy, organisation, planning, implementation, monitoring, measuring and improving best practice compliance measures. It follows the plan-do-check-act method, an iterative four-step management method used in business for controlling and continually improving processes and products. A well-known example of this is the ISO (International Organization for Standardization) Standard 9001 – Quality Management Systems, which has been successfully employed by more than a million businesses around the globe.

Examples of compliance management system standards are Australian Standard AS 3806-2006 – Compliance Programmes, German Audit Standard IDW AS 980 – Principles for properly auditing compliance management systems and, most recently, ISO Standard 19600 – Compliance Management Systems, the first global compliance management system standard. The purpose of these standards is to provide guidelines or minimum requirements for all private and public organisations wanting to design, implement, maintain and improve effective compliance management systems.

But what is the fundamental difference between compliance management based on a stand-alone corporate compliance programme and compliance management based on a recognised management system standard? The main difference is transparency, confirmability and comparability. Whereas classic stand-alone programmes, despite the frequent high-gloss codes of conduct, are often opaque, rather poorly documented, bottom-up (ie, rather single-risk than values-oriented) fragmentary compliance efforts, compliance management systems based on public standards are transparent, top-down, driven by leadership, values and principles and are comprehensive and well-documented compliance management efforts.

Now this may, to some degree, be theory, but it makes a huge difference whether an organisation, private or public, re-invents the wheel of compliance on its own or whether it follows a structured, public, transparent, auditable and externally certifiable process. And it simply makes a huge difference in terms of effectiveness. This is because standards, such as, for instance ISO 19600, introduce defined terms (for compliance, compliance culture, compliance function, etc) so that everyone speaks the same language, sets out the key role of leadership, tone at the top and ethical values and explains what good governance in compliance management requires. Furthermore, the ISO standard explains in detail the responsibilities at all levels of an organisation, the planning, implementation and monitoring, measuring and continual improvement of the best practice compliance management processes and tools (from – again – best practice and standards-based risk management to training and finally to reporting by employees and third parties of concerns).

Interestingly, a comparison of major compliance management system standards shows that there is little difference between them when it comes to the principles of good compliance governance, the organisation and the processes. Good compliance governance explicitly or implicitly always includes the compliance function's direct access to the board, its independence from operational management, adequate organisational authority, and availability of appropriate resources. The standards equally all underline board and top management responsibility for compliance and the essential role of the right tone and good example they set. They also address the key role in day-to-day management of the compliance function, and the need for a written compliance policy, professional risk management (another area with quite some room for improvement), and specific organisational (clear and easy to understand regulations, credible and effective reporting mechanisms, etc) and procedural measures (targeted training, timely and meaningful support, effective audits, etc).

To conclude, it is time to rethink compliance management and to take it to the next level. An educated and reasonable approach is to implement a standards-based compliance management system. By doing this, management adopts the same approach in compliance management that it has most certainly adopted in one way or another in its operative management of product or service quality. Following a transparent and recognised process, is – in general and in the long run – more effective and certainly less costly (including in terms of the cost of non-compliance) than a stand-alone, 'invented here' approach to compliance management. All organisations, but in particular small and medium-sized organisations, will appreciate the low cost of information on the principles of best practice compliance management and the simplifications associated with doing what many others do in the same manner. Effective compliance management will thus in future be easier and overall cheaper for all organisations, both private and public. And this is certainly a considerable gain for the sustainable management of businesses and for good public management.