Risk and compliance management systems

Daniel Lucien Bühr

Lalive

Best practice risk and compliance management – the questions boards and executive committees need to ask

Businesses introduce risk management processes and compliance programmes to ensure they handle (legal) risks adequately and comply sustainably and effectively with the law. Given the numerous fines imposed on leading businesses around the globe in recent years for repeated, 'systematic' infringements of the law, it can be assumed that risk management processes and compliance programmes in general fail to live up to their promise. As legal risks may constitute one of the largest business continuity risks, the shortcomings of current risk and compliance management should ring alarm bells for boards the world over.

On the assumption that corporate risk and compliance management are generally less effective than they should be (though evidence to the contrary is always welcome), the question immediately arises of whether there is a cure. One of the most prominent developments over the past few years has been the introduction of standardised risk and compliance management systems.

Management systems based on generally accepted international standards are an integrated process. They consist of a documented strategy, clear organisation, adequate planning, disciplined implementation, meaningful monitoring, accurate measuring of effectiveness and continual improvement. These systems follow the plan-do-check-act method, an iterative four-step management method used in businesses around the world 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 used by more than a million businesses worldwide. The key reason for applying standards-based management systems is that standardisation itself reduces complexity and cost and harmonises technical specifications of processes, products and services, which increases transparency, comparability and efficiency. For these same reasons businesses worldwide apply generally accepted accounting standards.

Effective risk management is a prerequisite for effective compliance management. Without a reliable process for identifying, analysing and evaluating risks and subsequently treating them, any business (in fact, any organisation) is eventually likely to hit the iceberg that no-one on the command bridge ever saw coming. According to a recent report by the OECD (2014, Risk Management and Corporate Governance), ISO Standard 31000 has de facto become the world standard in risk management. It was published in 2009 and is the only independent global risk management standard (another key document, while not an international standard, is the COSO (the Committee of Sponsoring Organizations of the Treadway Commission, a private sector initiative) 2004 Enterprise Risk Management Framework).

ISO 31000 firstly establishes clear terms and definitions. For instance, 'risk' is the effect of uncertainty on objectives, 'risk attitude' is the organisation's approach to assess and eventually pursue, retain, take or turn away from risk, 'risk assessment' is the overall process of risk identification, risk analysis and risk evaluation, and 'risk treatment' is the process to modify risk.

Based on this clear set of terms and definitions, ISO 31000 recommends that (senior) management commit to effective risk management and provide a documented mandate for designing and implementing a framework for managing risk. Once introduced, the framework needs to be monitored, reviewed and continually improved. The ISO Standard provides detailed guidance on the risk management framework, on risk assessment and on risk treatment techniques and provides a multilingual risk management vocabulary.

The questions boards and executive committees need to ask to reassure themselves that their risk management is in line with best practice are:

- What is the business's risk attitude and is the attitude documented and transparently communicated?
- What generally accepted international standard or risk management framework does the business apply?
- What generally accepted risk assessment techniques are applied and why those specifically?
- What are the top five risks resulting from the risk assessment process and have detailed risk descriptions ('risk scenarios') been drawn up for the attention of the board and the executive committee?
- What risk treatment measures have been taken, how did they modify the risks, and did risk treatment give rise to any new risks?

Of course, there is much more to be said (and asked) about best practice risk management. Some key risk management mistakes are, for instance, the reliance on mere risk governance concepts (which do not explain anything about risk management in a technical sense) instead of genuine risk management standards and frameworks; the (mal)practice of multiplying likelihood with consequences of an event or development, whereby worst case scenarios are factored out; or the massive underestimation of developments (for instance climate change) compared to one-off events. Still, by asking the above questions, any board or executive committee can quickly assess where their risk management stands in comparison to best practice.

The standards-based management system approach also applies to best practice compliance management. 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, since 2014, 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.

The fundamental difference between compliance management based on a stand-alone corporate compliance programme and compliance management based on a recognised management system standard 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, single-risk rather 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 systematic compliance management efforts.

In practice, it makes a huge difference whether a business or a public organisation reinvents the wheel of compliance management on its own or whether it follows a structured, public, transparent, auditable and externally certifiable process. Following an 'invented-here' concept costs more and it less effective.

ISO 19600 introduces defined terms (for instance 'compliance', which means meeting all the organisation's compliance obligations, '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 the detailed 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 the mechanism for the reporting of concerns by employees and third-parties).

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 all equally 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, effective risk management, 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).

The questions boards and the executive committees need to ask to be assured that their compliance management is consistent with best practice are:

- Are the ethical values of the company or organisation documented and consistently and visibly communicated top-down?
- What generally accepted international compliance management system standard or compliance management framework is applied?
- Is the compliance function independent and does the compliance function report to the board in the absence of executive committee members or other superiors at least once a year?
- What are the key compliance management processes and how are they systematically integrated into the operational processes?
- How is the compliance management system independently (internally or externally) monitored and measured for effectiveness and continually improved?

To conclude, it is time to rethink risk and compliance management and to take them to the next level. An educated and reasonable approach is to implement standards-based risk management and compliance management systems. By doing this, management adopts the same approach in risk and 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 generally accepted management 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 standalone, 'invented here' approach to risk and compliance management. All organisations, in particular multinationals but also risk-exposed small and medium-sized businesses, will appreciate the low cost of information on the principles of best practice risk and compliance management and the simplifications associated with doing what many others do in the same way based on generally accepted international standards.

Effective risk and compliance management will, in the future, be easier and overall less costly for all organisations. And this is certainly a considerable gain for the sustainable and diligent management of businesses and for good public management.