www.compliance-berater.de

Compliance Berater

1–2 / 2017

Betriebs-Berater Compliance

25.1.2017 | 5.Jg
Seiten 1–44

Beiheftet 1/2017 Compliance Across Europe

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

norm, the wording has to be changed from "should" to "shall" and reduced in length. Moreover, any examples provided must be excluded.
As the ONR 192050 is a requirement norm, the certification scheme results directly from the text of the norm. Regarding ISO 19600, the aforementioned approach to the guideline standards was applied by Austrian Standards to establish the certification scheme for ISO 19600. Currently, there are two valid certificates issued by Austrian Standards on conformity assessment of CMS: one for ONR 192050 alone and one for both ONR & ISO 19600. I served as lead auditor in both certification audits and the surveillance audits one year after the certificate was issued. One holder of a certificate is a regional energy provider with a majority of public shareholders. The second holder of the certificate is a section of the administration of the City of Vienna. Both organisations have published their certificates on their web-pages and the certificates are registered in the official certification register of Austrian Standards.
In conclusion, I would like to share with you some experiences of these certification audits and the principal benefits of a certification. The main effects observed from the audit process are increasing awareness of the importance of compliant behaviour for the organisation and effective communication from the top. Due the considerable numbers of people involved in the audit through interviews or observations of their day-to-day tasks, the audit is well-known throughout the organisation. The certificate is used for external stakeholders to demonstrate commitment to business activities in compliance with applicable regulations. Referring to the example given at the beginning of my contribution: a small and medium-sized company is faced with numerous requests from its suppliers to demonstrate the approach to compliance. A certificate may not replace or substitute due diligence by the business partner but it may positively influence the extent of such investigation.
The external audit process provides a summary of information to management about the status quo of the organisation's CMS in comparison to an international best practice benchmark. Last but not least, the three-year certification cycle under the ISO scheme ensures a structured approach to continual improvement of the CMS.

Cross-Border Compliance Standardisation – A Swiss NGO Perspective

Daniel Lucien Bühr*

I. Introduction

Switzerland has always been an active member country in international standardisation bodies. This is because Switzerland, with its small domestic market, has a vital interest in accessing foreign markets and ensuring low technical barriers to do so. With the increasing importance of cross-border services, the interest in international standardisation has also expanded beyond technical product standards and, today, includes management system standards. Switzerland, through the Swiss Association for Standardisation SNV, has actively contributed to the establishment of "ISO 19600 – Compliance Management Systems" and is also actively involved in e.g. "ISO Technical Committee 262 – Risk Management". Today's globalised economy would not have developed without international standards. Many aspects of our life are based on international standards, from the DIN A-4 format to "ISO 9001 – Quality Management" and the international financial reporting standards (IFRS). It is evident that standards are necessary to reduce complexity and cost for companies and individuals and to abolish barriers that would otherwise restrict trade, development and prosperity. The same goes for management system standards for risk management and compliance management. "ISO 31000 – Risk Management" and ISO 19600 are two key standards for best practice risk and compliance management. They are the only international standards in their field (if one defines a standard as a generally accepted description of the state of the art which has been developed by an independent standardisation body in an open, transparent process and by consensus). Of course, there are many guidelines and frameworks available for risk and compliance management. However, none of the organisations issuing such guidelines are independent nor are their standards generally accepted by all members of society, nor are their processes entirely open to all interested persons. Therefore, the availability of international standards for risk and compliance management is an important step towards better management of compliance risks and a chance for global uniform best practices resulting in a significant reduction of complexity and cost.

II. Standards are, by nature, genuinely cross-border and cross-cultural

The way international standards are developed (for instance by the International Standardization Organization ISO), is genuinely cross-border and cross-cultural. ISO Standard 19600 was developed by experts representing 11 member countries from America, Europe, Asia and Australia. The almost 30 experts were delegated from their national standardisations organisations to participate in the ISO project committee. During a period of 2 ½ years more than 1,000 comments on the draft standard were discussed and accepted or rejected in the consensus process. Thus, by the very way international standards come to existence, they represent what international experts view as being the state of the art in a particular field. Clearly, international standards are not free from error. However, they are reviewed every couple of years and, during this review process, comments from all interested stakeholders are considered (again by consensus). Looking at the process of international standardisation, it quickly becomes clear that no state, government or company (however big and powerful) can outperform an international standard on its own. A single organisation can never be as independent, international, multicultural and inclusive as the ISO, for instance. Moreover, given the cost associated with the individual exercise of re-inventing the wheel, it becomes evident that organisations should make use of generally-accepted instruments whenever they are available (such as international standards). Failing to do so results in a waste of financial and human resources and sub-optimal management effectiveness.

III. To effectively promote compliance, access to know-how must be low cost and easy

International standards are particularly important – if not vital – for small and medium-sized organisations, including governments with limited resources. They cannot afford to create their own way of doing things and they may lack technical expertise. Imagine a regulator in a poor country who wishes to understand what the current state of the art in compliance management is for the supervision of its banks, insurance companies and asset managers. With a few hundred USD, government officials can buy the relevant standards and get access to information that would easily cost a few million USD and a lot of human resources to (sort of) establish on their own. Furthermore, when government officials decide to incorporate international standards into their regulatory framework they use the same terms and speak the same language as their counterparts in other countries. They can even ask them for advice and exchange experience over time.
What applies to small and medium-sized organisations and developing countries also applies to large organisations, rich countries and their agencies. They are not able to create a true standard either and, in terms of resources, it also makes no sense for them to re-invent the wheel. After all, imagine the cost that would be saved if all companies of a regulated sector were required to choose one single standard (e.g. ISO 31000) for their risk management system. From a domestic and especially global point of view, the reduction of complexity and cost for organisations, for regulators and for external auditors (who would then review and certify standardised processes), could easily amount to tens or even hundreds of billions of USD per year. Money that is currently wasted.

IV. Public organisations and standardisation

International standards for management systems are addressed to all organisations, private and public. Public organisations should assess and treat their risks and manage compliance with the same diligence as any private sector company or NGO. Since public organisations generally act under parliamentary supervision, they are careful to maintain their independence – particularly from certain industries and foreign governments. Against this background, it is evident that the public sector can only apply independent and generally-accepted standards. A German regulator will most likely not apply or require companies to apply guidelines issued by a US regulator, for instance. And a Swiss regulator or agency would not be able to apply guidelines developed by a business association when assessing a compliance defence argument raised by a company under investigation. Under such circumstances, regulators can only apply independent national or international standards.

* *Daniel Lucien Bühr*, Member and lecturer on compliance management systems with the Swiss Association for Standardization/SNV, Vice-Chair Ethics and Compliance Switzerland/ECS and Partner at law firm LALIVE, Zurich. The views expressed are personal views and do not necessarily represent the views of SNV and ECS.

By way of example, the Swiss Confederation applies ISO 31000 across the board in the Federal Administration for risk management. The Swiss Competition Commission refers to ISO 19600 (among other guidelines) as a benchmark to assess whether it should accept a company's compliance defence and reduce a competition sanction because the company acted diligently in designing, implementing, maintaining and continually improving its compliance management system.

V. Standards strengthen sound principles, good governance and foster accountability

Standards are, by nature, based on principles. ISO Standard 19600 is a 30-page document. This is a very short guideline for a topic that could easily fill thousands of pages if one goes into details. However, the principles matter more than the 1,000 details and 10,000 rules you can imagine. In practice, it is usually the case that organisations get the principles wrong rather than the details. ISO 19600 is centred on leadership, ethical values and culture. They are the key drivers of effective compliance management. If an organisation decides to allocate resources to compliance but top management does not lead by example and is not seen to comply in the organisation, then every dollar spent on compliance is a waste of money. It is not a coincidence that almost all material integrity and compliance crises have resulted from a lack of leadership, values and culture. Therefore, one needs to get this right before starting to spend time and money on day-to-day compliance management. This underlying concept is stated clearly throughout the entire ISO Standard. The same goes for the implementation of a good compliance governance framework. Unless the compliance function has direct access to the board, is independent from line management and is given appropriate authority and adequate resources, every single dollar and every hour spent on compliance management will be of little use or even useless, depending on how severe the governance failure is. Standards also foster accountability because they demand clear and documented functional tasks and responsibilities, which must be measured and audited for effectiveness and be subject to regular reporting to top management and the governing body. Any organisation without clear functions and functional accountability is prone to risk and failure.

VI. Summary

Many organisations complain about too much regulation and demand less regulation. However, what they should really be demanding is more global standardisation of regulation which, in itself, would reduce regulatory complexity and cost to the maximum. Systematic risk and compliance management are topics which, for a few years now, have been outlined in international standards, particularly in ISO Standards 31000 and 19600. Organisations are free to apply international standards or other guidance or no standards or guidance at all. Not following a generally-accepted international standard is an option but clearly a bad, expensive and risky one. Organisations following a multitude of guidelines or following an "invented-here" approach inevitably spend more time and money on developing a framework which, by its very nature, will not be able to match the quality of an international standard. However, it is not only a waste of resources to re-invent the wheel but also a receipt for sub-optimal effectiveness and increased risk, for a lack of transparency and expensive follow-on costs (for instance for educating the auditors and new employees on what exactly one is doing). Imagine the financial savings and improvement in effectiveness that could be gained if all regulated financial institutions in the world were to apply a small number of generally-accepted international standards: all professionals would speak the same technical language, they would respect the same principles and apply the same practices and it would be transparent and easy to understand for employees, auditors, investors and regulators. The gain in effectiveness and the savings achieved by the reduction in complexity and cost would certainly be massive, to say the least. The positive result would certainly be comparable to the well-known result of applying generally-accepted accounting standards as opposed to the situation that existed up to the 1950s, where every organisation essentially had its own individually-accepted accounting standard. Therefore, it is time to think and act big and move forward to a less complex, less expensive and more effective risk and compliance management based on international standards. All organisations should act *now*: companies, governments and NGOs, for their own and their employees' benefit and also for a better society.

Introducing Compliance to the Shop Floor – ISO 19600 and Germany

Michael Kayser*

When the International Organisation for Standards published the ISO 19600 Compliance Management Standard in late 2015, the reaction throughout Germany was scepticism to harsh critique in some compliance quarters. Critics questioned how the organisation responsible for technical standards could concern itself with a largely legal topic. "Amateurs vs. professionals" was the tag line on the one hand, "Nothing new here and therefore not required" on the other. Initially, the compliance profession's scepticism outweighed the curiosity that should have been warranted. This reaction may not be as surprising as it seems, given the development of compliance in Germany in the past. Understanding the history of compliance, and how Germany got to where it is today, may explain some of the controversy surrounding the reaction towards the standard.

I. Compliance in Germany

Germany has had its fair share of high-profile compliance cases, with a prominent case 2006 when Siemens got into trouble, closely followed by major breaches within Daimler, Deutsche Telekom, and Deutsche Bahn among others. These compliance cases where rigorously prosecuted with hefty fines being imposed. Consequently, calls for protective measures were made – particularly from and in relation to the supervisory boards and their potential liabilities. The call for compliance management systems grew stronger and (at least within large, publicly listed organisations), significant investment went into establishing related structures. Against this background, it is no surprise that the people charged with establishing and maintaining those structures came from a predominantly legal background, having previously been lawyers and solicitors or involved in internal audit or finance.

In the years that followed, compliance established itself as a predominantly legal concept affecting organisations, starting with the large, publicly listed companies. During this period, the focus started shifting from purely defensive characteristics to the implementation of preventative measures. At the same time, compliance requirements found their way into supply chain relationships, increasingly affecting the "*Mittelstand*" (i.e. organisations still considerable in size, but neither listed nor publicly owned). Over time, these developments contributed to a considerable level of compliance awareness and maturity in Germany.

II. Operational and Legal Aspects

Interestingly enough, it could be argued that promotion through supply chain relationships and the increasing focus on preventative measures saw organisational and operational aspects starting to move into the foreground, adding to the originally legal risk. Therefore, it seemed natural for standards organisations to step up to the challenge and get involved, particularly in relation to management system standardisation. Approaching compliance from an organisational and operational perspective can even be characterised as the point when it arrived in the day-to-day business world, offering the chance to make it mainstream – somewhat like to the concept of quality in the mid-80s.

III. The Approach

In developing ISO 19600 (and as with earlier management system standards), the aim was to provide guidelines and guidance for organisations that wished to firmly implement compliance in their respective organisations. In developing this concept, nothing radically new was invented. Rather, the work involved taking various concepts, guidelines and principles that existed locally to a certain level of detail, such as the national standards of Austria and Australia, general worldwide principles (as formulated by the UN Global Compact) and various other initiatives (e.g. the ones published by the OECD). In its development, it incorporated experience already gained over the past few years, including that of compliance-mature environments. Consequently, the result reflects rather than contradicts existing practices, adding an operational dimension and (most importantly) a universal international understanding of the concept of a compliance management system. From a German perspective, it translated a legal view into an operational, management system- based approach.

* *Michael Kayser* is a seasoned professional with over a decade experience in high-stakes, mission critical technology based services. A veteran of the e-learning and assessment industry, he leads market leading compliance services provider Idox Compliance now.