Appeared in Ethic-Intelligence Expert's Corner / Newsletter:

http://www.ethic-intelligence.com/experts/16945-iso-19600-first-international-standard-compliance-management-systems/

ISO 19600 on compliance management systems: how can it help organizations?

Daniel L. Bühr

Partner, LALIVE

Zurich

What should a diligent manager consider when it comes to legal risk management?

The reasons for applying standard-based management systems are that standardization reduces complexity and cost whilst increasing effectiveness. Businesses introduce risk and compliance management systems to make sure that their (legal) risks are treated effectively. On top of that, organizations and managers that are suspected of not meeting all their compliance obligations are increasingly exposed to merciless public criticism and strict government enforcement action. This is the reason why a diligent manager should focus on the establishment, implementation, evaluation and continuous improvement of a best practice compliance management system. Indeed, for any type of business, best practice compliance management creates a competitive advantage and for public organizations it constitutes the core of good public governance. Some key risk management mistakes are the reliance on mere risk governance concepts (such as the Three Lines of Defence concept), thereby not addressing genuine risk management on substance, as is the case in ISO 31000.

What is ISO Standard 19600 and how can it help organizations to increase the effectiveness of their compliance management?

ISO Standard 19600 – Compliance management systems provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization. It is the one and only independent, international standard for compliance officers, businesses, regulators and judges.

The guidance is adaptable to any organization and can be of use with regard to any compliance risk. Furthermore, it is adjustable to the level of maturity of an organization's

compliance management system and to the nature and complexity of the organization's activities. After defining the key terms to establish a common compliance language, the standard recommends that the context of the organization be established, in particular its compliance obligations. The implementation of principles of good governance is equally important for the effectiveness of the system. Only if the compliance function is independent (including direct access to the board) and has the authority and resources needed can it do the job. Another key element is best practice risk management, which shall essentially identify the risks originating from a delta between compliance obligations and the organization's meeting of the latter. The assignment of clear management responsibilities ensures that at all levels of the organization everyone knows his/her compliance responsibilities and rights. The following processes allow for the successful achievement of compliance with all obligations, which is the standard's ultimate goal: performance evaluation, compliance reporting, operational planning, training, internal instructions, measurements, audit and reporting as well as continual improvement. In sum, following generally accepted management system standards is in the long run more effective and less costly (including in terms of the high cost of non-compliance) than a stand-alone, plucked out of the air approach to risk and compliance management. Furthermore, businesses and public organizations will appreciate the low cost of information regarding the principles of best practice risk and compliance management as well as the transparency and comparability of their management system.

Is the implementation and maintenance of a compliance management system costly? Is it a worthwhile investment?

Compliance itself is not merely an operational cost, but also an investment in an organization's future and an essential element of the diligent management of any organization. If one believes that the cost of compliance is high, imagine the costs of non-compliance and the rather unpleasant impact on the reputations and career perspectives of the managers and employees.

What is the relation between ISO 19600 and ISO 37001?

ISO 37001 specifies requirements and provides guidance for establishing, implementing, maintaining, reviewing and improving an anti-bribery management system. The system can be stand-alone or can be integrated into an overall compliance management system. This new standard requires the organization to implement a series of best practice measures, such as an anti-bribery policy, leadership, the appointment of a person to oversee anti-bribery compliance, personnel training, bribery risk assessments, due diligence on projects and business associates, the implementation of financial and commercial controls as well as reporting and investigation procedures. While ISO 19600 is the comprehensive compliance management system standard, ISO 37001 specifically addresses anti-bribery compliance risks through the establishment of a set of

requirements. Of course, an organization which only meets the requirements of ISO 37001 will remain exposed to all other compliance risks unless it introduces a comprehensive compliance management system in accordance with, for instance, ISO 19600. In conclusion, it goes without saying that the combination of both standards allows an organization to build a robust overall compliance management framework.

The ISO 19600 Commentary elaborated by members of the ISO project committee is about to be published and can be ordered at the following link. How does this commentary assist professionals working in the compliance sector in establishing a best practice compliance management system?

The commentary assists board members, management at all levels and compliance officers through best practice insights and recommendations from field experts and showcases examples of their daily compliance work. The commentary provides the "tips and tricks" necessary to implement a tailored compliance management system whilst being in line with tested best practices.

Daniel Bühr co-authored the ISO 19600 Commentary with Martin Tolar. It is available from LexisNexis at the following link: https://shop.lexisnexis.at/iso-19600-compliance-management-systems-9783700762195.html.

Daniel L. Bühr

Partner, LALIVE

Stampfenbachplatz 4

P.O. Box 212

8042 Zurich, Switzerland

Email : dbuhr@lalive.ch

November 2016