comply.

DR. FRANK HERDMANN RECHTSANWALT
AUXILIUM MANAGEMENT SERVICE

Abstract of an essay in edition 01/2016 of comply., the journal for compliance officers, pgs. 38 ff

The risk based approach in ISO 19600 and risk management in line with ISO 31000

HOW COMPLIANCE RISKS CAN BE MANAGED WITHIN A RISK MANAGEMENT SYSTEM ALIGNED WITH ISO 31000

Reproach addressed at ISO 19600

ISO 19600 is said to claim following a risk based approach while missing to give sufficient guidance on risk management. This reproach will be shown wrong in view of the reference to ISO 31000. Risk management aligned with ISO 31000 can be used as a link between all management systems of an organization complementing the recommendations and requirements of specific management system standards. The standards are interlinked making requirements for management easier to handle reducing efforts in particular for small and midsize companies.

Prae ISO 19600 and ISO 19600 as a management system standard

In the past it was discussed whether compliance is just a new term or a new challenge. Pointing out that in a complex world a systematic approach is required, the development of a compliance program, like the three column model, was demanded. ISO 19600 issued in 2014 gives guidance on the introduction, development, implementing application and continual improvement of a compliance management system. It follows structure and terminology of the ISO rules on Management System Standards which are facilitating integration into an unified holistic management system.

Risk based approach and ISO 31000

Compliance obligations of the organization have to be identified and documented and related to all its activities and aspects of its operations in order to identify, analyze and evaluate compliance risks. This is called the »risk based approach«. The organization is free to use a more formal or any other suitable approach for risk assessment, but reference is made to the guidance that can be found in ISO 31000. In its principles ISO 31000 notes that an effective and efficient risk management is an integral part of all organizational processes. The risk management process as described in clause 5 should be embedded in the culture and practices and tailored to the business processes of the organization.

Management of compliance risks based on risk management

The core risk management process comprising risk assessment and risk treatment including monitoring and documentation resembles a loop that should be integrated into any activity of the organization like a plug-in IT-dongle facilitating an enhanced performance. Naturally this applies for any activities within the Compliance Management System of the organization – whether they are formally designed and documented processes or not. Risk Management is part of the responsibilities of management (including top management) and everybody who belongs to the staff. It is not a standalone activity – this is the end of silo risk management.

The full text of the essay (German) for download: [PDF]

For more information contact the author: dr.herdmann@auxiliumservice.de
Dr. Frank Herdmann | Gluckweg 10 | 12247 Berlin | Germany | phone: +49 30 771 90 321