Austria: ISO 19600: Compliance Management Systems - Guidelines

As a young and complex matter, compliance presents numerous challenges for organizations. This is partly due to the lack of global standards, which could provide guidance. As a consequence, organizations are having a hard time recognizing those compliance requirements that are necessary, appropriate and capable of serving as indicators of a functioning Compliance Management System ("CMS"). Therefore, it is highly welcome that the International Organization for Standardization ("ISO") is currently working on a global standard for CMS.

The participating ISO members had the chance to comment and vote on the draft of ISO 19600 until April 2014; they endorsed the draft unanimously. The competent committee (ISO/PC 271) is currently meeting in Vienna to review the comments and votes and then issue a final draft based on their review. The final draft will be put up for a final vote. Provided that the final vote will be positive, ISO 19600 will presumably be published in 2015.

ISO 19600 (the current draft is available online) is designed as a flexible guideline without any normative references. It provides recommendations based on the principles of good governance, flexibility, proportionality, transparency, and sustainability. It is open for all kind of organizations. Especially small and medium-sized companies benefit from this approach, as they can implement the guideline recommendations according to the size and maturity of their company. It is this kind of flexibility that gives small and medium-sized companies the incentive to deal with compliance on their own terms. Because the guideline is based upon the principle of continual improvement (plan, do, check, act), organizations can expand their CMS as their needs increase.

Since ISO 19600 follows the ISO "High Level Structure" ("HLS"), it can be implemented in already existing management systems that are using the HLS standard. Since ISO 19600 follows this HLS, it can serve as an additional module for those companies having already implemented ISO's quality management standards according to ISO 9000 et seq. This approach makes it easier and therefore more likely for companies to implement the CMS measures recommended in ISO 19600.

The ISO 19600 guideline also follows a risk-based approach. After establishing the context in which it operates, the organization must perform a compliance risk assessment. The identified risks (compliance obligations) are the basis for establishing and implementing controls. The performance of those risk treatment measures must then be evaluated and improved upon, as well as communicated both internally and externally.

The structure of ISO 19600 focuses on the different stages of CMS integration from development to implementation, evaluation, maintenance, and continual improvement. After determining the objectives and the scope of the CMS, the guideline recommends the appropriate measures in accordance with stakeholder interests and good governance.

The guideline emphasizes the different roles, responsibilities, and authorities within the organization and focuses on the establishment of a compliance policy. By doing so, it aims to create an organizational culture in which compliance becomes the general rule – a compliance culture, so to speak.

The ISO standard also recommends measures for establishing controls and procedures to achieve the desired behavior. The recommended measures should be accompanied by trainings, internal and external communication, documented information, and the top management’s encouraging behavior. Finally, ISO 19600...
pays attention to performance evaluation and improvement upon noncompliance, especially in terms of the escalation process. The recommended measures for noncompliance (react, evaluate, implement any action needed, review effectiveness, make changes if necessary) do quite a good job of illustrating the principle of continual improvement.

**Comparison to ONR 192050**

In 2013, the Austrian Standards Institute released its very own standard for CMS, called ONR 192050. The ONR specifies minimum standards for the development, introduction, and maintenance of a CMS. Since it sets up requirements for a certification, the ONR standard is far less detailed than the ISO standard. Furthermore, its scope is narrower than that of ISO 19600. ONR 192050 is only applicable for the observance of statutory obligations that are binding on the organization, whereas ISO 19600 applies with regard to all requirements that an organization must or chooses to comply with.

Both standards are applicable to organizations of all types and sizes. Therefore, they also take into account the organization’s size and risk situation. Nevertheless, it is striking that the Austrian ONR focuses mostly on the role of the organization’s top management and compliance officer (whose tasks can be performed by any organization member), while the ISO guideline aims to create a compliance culture within the organization by establishing a compliance policy and including all employees.

Other than that, ONR 192050 sets out very basic requirements for the assessment, documentation, monitoring, and handling of compliance risks, such as "A procedure shall be defined for following up on breaches of regulations detected", while ISO 19600 recommends as to such procedure that "(t)he process should specify to whom, how and when issues are to be reported and the timelines for internal and external reporting."

The combination of ONR 192050 and ISO 19600 works well. Still, the ONR should be adapted according to the ISO, especially with regard to its scope and the definition of terms, so that the national standard can provide requirements for a certification, while the international standard can provide guidance by recommendations. Nevertheless, it is important to emphasize that an already implemented CMS according to ONR 192050 does not have to be changed to comply with ISO 19600. There is no evident conflict and even if that were to be the case, the ISO standard would be compatible with other compliance measures, as long as they lead to the same result.

**Comment on ISO 19600**

The flexible approach of ISO 19600 is noteworthy. Every organization can decide independently to what extent the implementation is still deemed proportional (with regard to the involved costs and benefits). The structure combined with the overlying principle of continual improvement enables organizations to act in accordance with ISO 19600 in every stage of their CMS-development and to improve upon it.

A global standard will add comparability between compliance systems in different jurisdictions and industries. The guideline can be used globally due to its broad scope and its character as a recommendation-only standard. In addition, the guideline brings with it no risk of a conflict with any national law.

However, it is still unclear how organizations are supposed to prove their implementation of the ISO recommendations to others. Currently, there is no intention of establishing a certification according to ISO 19600, since there are no
provided minimum standards. This is the downside of a flexible guideline that tries to cover a broad spectrum. In addition, there are national standards for CMS, such as the Austrian ONR 192050, which provide certification if their minimum standards are met. These national standards are not (yet) harmonized with ISO 19600. Therefore, it can occur that a Compliance Officer is confronted with conflicting provisions, especially since the definitions are inconsistent. This is not harmful per se, since ISO 19600 is compatible with other compliance measures, but it still counteracts the aspired global standardization. This point should be tackled in order to create a global standard. Since there is no majority to be found amongst the ISO members for establishing a certification according to ISO 19600, at least the national standardization institutes should coordinate and adapt their respective national CMS standards structurally and conceptually to ISO 19600. However, the ISO’s approach could change. In case the ISO members find a majority for certification (or at least an affirmation to comply with the guideline) according to ISO 19600 might be possible in future.

Conclusion

All in all, ISO created a solid guideline that stands out for its flexibility. Because of its global comparability, the ISO standard can have a positive impact on business. Business partners can demand implementation of the recommended measures and thereby create a (soft) obligation to uphold the ISO standard. This approach already worked well with corporate governance measures. The guideline could be applied as a module to adapt an existing ISO-certified management system of an organization.

A unified certification would be desirable, though it seems there is currently no majority for such a development amongst the participating ISO members. Therefore, at least the national standardization institutes should adapt their respective national CMS standards to provide unity. Still, we are positive that the future will show that there is a demand for a certification (or affirmation) according to ISO 19600 to manage compliance matters systematically.