

Do DOJ Policy and ISO Compliance Standard Overlap; and What Are the Pros and Cons For Applying the ISO Standard?

by **Daniel Lucien BÜHR**

In February 2017, the Fraud Section of the United States Department of Justice's Criminal Division published a document entitled "Evaluation of Corporate Compliance Programs." This document lists the assessment criteria for effective corporate compliance programs. The DOJ recognises that each company's risk profile and the solutions it adopts to reduce risks should be evaluated on their own merits. The DOJ therefore tailors its determination to each case. However, even tailored determinations raise many of the same questions. The DOJ document explains the questions the DOJ may ask about a corporate compliance program. However, it gives no guidance on how companies can actually provide the right answers.

In December 2014, the International Organization for Standardization published ISO International Standard 19600 – Compliance management systems – Guidelines, which helps organisations establish, develop, implement, evaluate, maintain and improve an effective and responsive compliance management system. It is the first international standard on state-of-the-art compliance management and provides the conceptual basis for other international standards, such as ISO 37001 – Anti-bribery management systems.

The DOJ document and ISO Standard 19600 differ, yet they have a shared preventive goal. A comparison between the DOJ document and the ISO Standard 19600 shows that US policy and the Standard are largely compatible, and that ISO 19600 is an appropriate tool for companies to get to a level of compliance management that allows them to provide the right answers to the DOJ's questions, should that be necessary: [Risk and Compliance Management \(PDF: 296 KB\)](#). The table in the comparison illustrates the overlap between the DOJ and ISO guidance; the flowchart opposite the table illustrates the iterative "plan-do-check-act" management system that the Standard advocates. The colour scheme of both graphics indicates the topical overlap.

Now what are the pros and cons for applying the ISO standard? As all standards, the ISO Standard 19600 has the purpose of consolidating global best practice, creating transparency and reducing complexity and cost. Just imagine the reduction in cost that could be achieved if globally all banks

followed one single method for compliance management. Transparency, comparability, auditability, and effectiveness would increase significantly and costs for access to information/know-how, tools, external audits, regulatory reporting and supervision by regulators could be saved and would become available for currently under-resourced compliance tasks like anti-money laundering compliance. Every aspect of our lives is based on standards, and without international standards no smartphone would work and no car would be up to today's safety requirements.

The ISO Standard 19600 was developed by 30 experts, representing the participating national standardization organizations. In a two year process the project committee circulated two drafts and discussed more than 1,000 comments submitted by the participating national member organizations of ISO. The ISO standardization process is based on the consensus principle and is inclusive, democratic and independent. As a matter of fact, no single state or corporation would probably ever be able to replicate the ISO standardization process and develop an equally authoritative standard.

In my view, the ISO Standard 19600 has clear advantages to the available compliance models (such as the Three Lines of Defense Model) or various guidelines from international organizations such as the OECD or the ICC: In addition to the advantages of its development process, the ISO Standard is based on a tested management system approach (ca. 1.5 million companies apply and are certified under ISO management system standards). ISO 19600 is based on a systematic management cycle which covers good governance, risk management, leadership, and roles and responsibilities at all levels, planning, support, operation, performance evaluation and continual improvement. On substance, the thread of the standard is that the leadership, values and culture drive organizational compliance. The Standard defines the relevant terms (compliance, for instance, is meeting all the organization's compliance obligations, specifically the compliance requirements and the compliance commitments), sets-out the good compliance governance principles (direct access of the compliance function to the Board, independence and the allocation of appropriate authority and adequate resources to the compliance function). The standard then is clear about the coaction with risk management, the roles and responsibilities for compliance from Board level to the employees, it describes in detail the tasks of the compliance function, describes the training process, measurement of effectiveness, reporting, continual improvement etc. To cut a long story short, ISO Standard 19600 offers to all organizations a systematic way of managing compliance in line with international best practice, reflecting essentially all the topics that have been discussed in the global compliance community in the recent years: tone at the top, good compliance governance, speak-up and listen-to culture, solid processes, documentation, measurement of effectiveness, reporting etc. Besides: some parts of the standard are inspired by U.S. documents, such as the DOJ/SEC FCPA Resources Guide (for instance Section 10.1.2 on

reporting mechanisms/whistle-blowing). And as outlined in the article on the DOJ/ISO overlap, both concepts and benchmarks are astonishingly, or probably better: logically, coherent.

Now in practice, why in my view is the ISO Standard better than other compliance frameworks? The ISO Standard is better than the Three Lines of Defense Model or other guidance, because it is more than a (few pages) model or rather summary guidelines, it is a comprehensive management system. And it is modern because it focuses on the drivers of compliance: Leadership, values and culture and deals with key aspects of effective compliance such as the tone, action and visible commitment at the top, the independence of the compliance function, adequate resources, documented processes, measurement of effectiveness, reporting and escalation.

And what are the cons of the ISO Standard 19600 Standard? Honestly, I do not believe that there are real cons. The Standard is currently in the process of revision and there will certainly be improvements. Personally, I believe that consequences of non-compliance should be addressed in the revised Standard. And the Standard should in my view also consider compliance in the context of the digital transformation. But other than these aspects, my view is that ISO Standard 19600 is one of the best documents ever written on systematic and effective compliance management. And having been a member of the expert committee that drafted the Standard, I am of course entirely unbiased to make this statement. But more seriously, I am happy to discuss the pros and cons of using the ISO compliance management systems standards with the readers of this blog. And hopefully the one or the other reader will join the Working Group 4 of ISO Technical Committee 309 (Governance of Organizations) and contribute to the forthcoming revised Standard.

Daniel Lucien BÜHR is a partner at LALIVE.

Disclaimer

The views, opinions and positions expressed within all posts are those of the author alone and do not represent those of the Program on Corporate Compliance and Enforcement (PCCE) or of New York University School of Law. PCCE makes no representations as to the accuracy, completeness and validity of any statements made on this site and will not be liable for any errors, omissions or representations. The copyright of this content belongs to the author and any liability with regards to infringement of intellectual property rights remains with the author.

This entry was posted in Compliance and tagged Daniel Lucien BÜHR on November 14, 2018

[https://wp.nyu.edu/compliance_enforcement/2018/11/14/do-doj-policy-and-iso-compliance-standard-overlap-and-what-are-the-pros-and-cons-for-applying-the-iso-standard/] by Allison Caffarone.

Accessibility