Development of an ISO standard on compliance management

*Dick Hortensius, senior-consultant NEN Management systems, NEN, Netherlands*

**Background**

In 2012 Australia proposed to start the development of an ISO standard for compliance programs based on the national Australian standard AS 8306. This proposal has been accepted by the members of ISO and a Project Committee (PC) has been established to develop the standard. ISO/PC 271 “Compliance Programs” is chaired by Martin Tolar, president of the Australasian Compliance Institute and the secretariat is provided by the Australian standards body SAI.

Nowadays compliance management receives a lot of attention in a wide variety of business sectors. In the financial sector the presence of an independent ‘compliance officer’ is a well-known phenomenon for a number of years, comparable with the ‘controller’ for financial matters. But also in the non-financial sector the *Chief Compliance Officers* are entering, e.g. in building companies, the chemical industry and in energy generation and distribution. All these sectors have to cope with complicated legislation and regulations for which compliance is important with a view to safety and environmental risks but also with a view to business continuity and assurance of continuing delivery of vital services. Companies acknowledge that the basis for social responsibility is well organized and managed compliance with legislation as well as with the organization’s own ethical codes and corporate directives. Governmental authorities show an increasing interest in compliance management in companies. This may assist them in setting priorities in inspection activities (e.g. less frequent visiting companies with sound compliance management systems) and in the way they carry out inspections (making use of information that is resulting from the compliance management system).

**Broad approach to compliance management**

Compliance management is (much) more than just meeting the requirements of laws and regulations. Organizations have to deal with many different types of requirements from a variety of stakeholders (e.g. customers, sector organizations, etcetera), certificates and key marks that have been chosen on a voluntary basis and *last but not least* their own company rules and codes of business. These (ethical) codes are taking more seriously nowadays as a result of *corporate governance* and social responsibility. Management of all these different requirements is becoming more difficult, but also more important with a view to liabilities, public image and the ‘license to operate’. Often the responsibility for managing compliance with specific requirements is delegated to different persons and departments within the organization. Technical requirements (customer specifications and technical regulations) are the responsibility of operational management, general laws and legislation are covered by legal or external affairs and the internal rules and codes of conduct are the responsibility of the HRM department and Internal Control. As a consequence management of requirements will differ; there is potential overlap or matters are falling between two chairs. Technical requirements are controlled with technical measures of which the integrity has to be maintained (maintenance, effective procedures and work instructions, competence of personnel). However, in case of compliance with codes of conduct/ethics, directing the attitude of people and creating the right culture is more important. The Australian proposal for an ISO standard covered this broad scope of compliance management.
**First working drafts**

In preparation of the first meeting of ISO/PC 271 in April 2013 a working document has been circulated in which the content of the Australian standard AS 3806 has been merged with the core text and structure of ISO management system standards. The advantage of this approach is that compliance management can easily be integrated with other management systems that are based on ISO standards (e.g. environmental management according to ISO 14001 and quality management according to ISO 9001). The disadvantage might be that the standard then also describes a range of generic management system elements (e.g. document control, internal audit, monitoring and measurement, management review) where the focus should be on elements that are specific for effective compliance management.

![Figure 1 – Plug-in model for ISO management system standards](image)

**ISO/CD 18386** Compliance management systems

During the first meeting of ISO/PC 271 two important decisions have been made that determine the content and format of ISO/CD 18386:

a) It will be a guidance document and not a specification (requirements standard);

b) It will describe a compliance management system.

The first decision implies that ISO 18386 is not intended for certification, but provides organizations with ‘good practice’ that they can fully or partly implement. The second decision means that the standards will be aligned with the new core text and structure of ISO management system standards.

---

1 This number will be changed in future to ISO 19600
standards. Therefore ISO 18386 will be a ‘plug-in’ for compliance management in the integrated management system of the organization (see figure 1). Herewith an organization can enhance the compliance elements in e.g. its environmental and quality management.

In the box two key definitions from the Committee Draft are included. These show that the scope of compliance management covers both legal and voluntary obligations.

**Box – Definitions in ISO/CD 18386**

**Compliance**: meeting all the organization’s compliance obligations

**Compliance obligation**: requirement that an organization has to or chooses to comply with

_Note - Obligations may arise from mandatory requirements, such as applicable laws and regulations, or voluntary commitments such as industry standards and codes, contractual relationships, principles of good governance and accepted community and ethical standards_

Determination of the compliance obligations and implementation of measures (controls) in the organization to ensure compliance with these obligations is a step-wise process. It starts with gaining insight in important external circumstances, conditions and factors: the context in which the organization operates and its stakeholders. Followed by the identification of compliance obligations and determining the compliance risk, i.e. probability and consequences of non-compliances with requirements. Finally, the organization should plan, implement and monitor measures to control the compliance risks. This process aligns very well with the High Level Structure for management system standards. In table 1 this structure is given with a general description of the specific guidance for compliance management as included in CD 18386.

<table>
<thead>
<tr>
<th>High Level Structure for ISO MSS</th>
<th>Guidance on compliance in ISO/CD 18386</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context of the organization</td>
<td>Analysis of the environment in which the organization operates (context, issues, stakeholders) Scope of the compliance management system Identification of compliance obligations Assessment of the compliance risks</td>
</tr>
<tr>
<td>Leadership</td>
<td>Policy, commitment, leading by example Roles, responsibilities and authorities with respect to compliance for the board, top and line management, employees and an independent compliance officer</td>
</tr>
<tr>
<td>Planning</td>
<td>Planning of measures to control compliance risks Establishing of compliance objectives</td>
</tr>
<tr>
<td>Support</td>
<td>Awareness, competence and training in compliance Behaviour and culture Communication and documentation</td>
</tr>
<tr>
<td>Operation</td>
<td>Implementation of controls for compliance (technical, procedural, directing the attitude and behaviour of personnel)</td>
</tr>
<tr>
<td>Performance evaluation</td>
<td>Monitoring of compliance, application of indicators Analysis of information and reporting of results (internal and external) Records management</td>
</tr>
<tr>
<td>Improvement</td>
<td>Actions on non-compliance of requirements and escalation to higher management levels when necessary Corrective action Management review and improvement activities</td>
</tr>
</tbody>
</table>

Table – Correspondence of the HLS with specific guidance on compliance management
**The further development process**

ISO member bodies were able to vote and provide comments on the *Committee Draft* by mid-August 2013. During the next meeting of ISO/PC 271 in October in Paris, it will be decided what the next step can be: issuing a Draft International Standard (DIS) or a second Committee Draft. This decision will depend on the results of the ballot and the nature of the comments provided. The Netherlands mirror committee would like to spend more time to discuss the basic elements of effective compliance management and how to provide clear guidance on risk-based approach to compliance management (see the annex). Additionally the Netherlands are of the opinion that more ISO members should be actively engaged in the development of this important guideline and therefore more time is needed to move to the stage of DIS.

**Stages standards development**

ISO 18386 compliance management

WD1: January 2013
CD 1: Sydney, April 2013
CD 2 or DIS: Paris, October 2013

Figure 2 – Standards development process

**More information**

More information on this subject can be provided by Dick Hortensius, +31 15 2 690 115, e-mail: dick.hortensius@nen.nl.
The risk-based approach to compliance management in ISO/CD 18386

Input of Netherlands to ISO/CD 18386

A risk-based approach to compliance management is important to ensure that it is aligned with and contributes to the policies and objectives of an organization and is focused on the most significant compliance risks.

The content and structure of ISO/CD 18386 provide a good basis for a risk-based approach; however, it can be strengthened and be made more explicit by applying the risk management process described in ISO 31000.

In the figure below parts of ISO/CD 18386 are related to the risk management process described in clause 6 of ISO 31000.

This figure illustrates that ISO/CD 18386, by following the High Level Structure for ISO management system standards, indeed contains the basic elements of the ISO 31000 risk management process, but also that an important step (i.e. risk evaluation) is missing, or at least not explicitly dealt with yet.
Following the terminology of ISO/CD 18386 and ISO 31000, **compliance risk** is the effect of uncertainty on (achieving) the compliance objectives of an organization. It is the risk of occurrence of non-compliances with the compliance obligations of the organization that it has identified in line with its compliance policy and objectives.

**Establishing the context** is an important basis for identifying the organization’s compliance obligations and establishing criteria to evaluate compliance risks.

**Identification of compliance risks** (the first step in the risk assessment) involves considering the compliance obligations and to relate these to activities, products and aspects of the organization, to identify situations and circumstances where non-compliances can occur.

**Analysis of compliance risk** involves identifying causes of non-compliance (compliance failures), likelihood of their occurrence and the severity of their consequences, as a basis for ranking or categorizing compliance risk (e.g. by applying a risk matrix).

**Evaluation of compliance risk** involves comparing the level of risk established in the previous step with the risk criteria established when the context was considered. Criteria should be established by taken into account e.g. legal requirements, stakeholder concerns and impact of consequences of non-compliances. Evaluation of compliance risks should assist in determining and prioritizing the implementation of controls (i.e. **risk treatment**). Compliance management is aimed at preventing all non-compliances, however, the extent to which controls are implemented for specific compliance obligations may depend upon the level of compliance risk and be based on the results of the compliance risk evaluation. Also, risk treatment measures are limited and a residual risk of non-compliance may remain after implementation. For these residual compliance risks and for situations with low compliance risks where little or no controls are implemented, **monitoring** will assist in identifying whether nevertheless non-compliances occur, that should be corrected, followed by corrective actions that can involve implementing (additional) controls to prevent re-occurrence of non-compliances. The types of indicators applied in the monitoring process can be derived from the risk assessment process.