

---

# ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

By Sylvie Bleker and Dick Hortensius\*

■ It has been a traditional complaint of the global compliance officer that regulatory expectations and standards of conduct are uncoordinated across borders, leading to conflicts of emphasis and inefficiencies in the implementation of global compliance programmes from one jurisdiction to another. Increasingly of concern has been also the requirement to verify and ensure that appropriate measures exist for ensuring compliant behaviour within major suppliers, distributors, and other agents deemed to be acting, even indirectly, on behalf of the firm. Whereas some regulators in certain industries have been quite explicit as to what constitutes an effective programme, others have been less articulate; and in many industries there is a clear lack of guidance on the subject at all. It could be that help is at hand, this time from the ISO (International Organisation for Standardization).<sup>1</sup> Even better, there is still time to influence its outcome. This article by Sylvie Bleker and Dick Hortensius provides background information on the reasons why this ISO standard was initiated, explains the content of the current draft standard and its relationship with other well known and widely accepted ISO standards and its significance for companies and governmental authorities.

## Background

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,

already in place for a number of years, comparable with the ‘controller’ for financial matters. But also in the non-financial sector the *Chief Compliance Officers* are making their entrance, e.g. in building companies, the chemical

---

\* Sylvie Bleker is the chair and Dick Hortensius is the secretary of the Dutch standards committee on compliance management that actively contributes to the development of ISO 19600. Sylvie is also Program Director of the Postgraduate education on Compliance & Integrity Management, and Chief Compliance & Risk Officer at Ballast Nedam, whilst Dick is a senior-consultant at NEN Management systems, Netherlands.

1 <http://www.iso.org/iso/home/about.htm>

### ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

*As a consequence of both differences in approach and departmental objectives, management solutions applied to meet (compliance) requirements will differ; there is therefore a potential overlap of concerns, or a risk that matters might fall between two stools*

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 integrity (e.g. anti-corruption, terrorist financing or money laundering) and related thereto, business continuity and assurance of the continued delivery of vital services. Companies acknowledge that the basis for the effective achievement of any social responsibility objectives is a well organized and managed compliance with rules and applicable laws, as well as with the organisation's own ethical codes and corporate directives. Government authorities show an increasing interest in the compliance management of companies. This may assist them in setting priorities for inspection activities (e.g. less frequent visits to companies with sound compliance management systems) and in the way they carry out inspections (making use of information that emanates from the compliance management system).

#### **ORIGINS OF THE ISO 19600**

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 was accepted by the members of ISO and a Project Committee (PC) was established to develop the standard. ISO/PC 271 "Compliance Management" is chaired by Martin Tolar, president of the Australasian Compliance Institute and the secretariat is provided by the Australian standards body SAI. After two meetings of this ISO Committee the Draft International Standard ISO 19600 "Compliance management systems - Guidelines" has been published for voting and comments by the members of ISO.

#### **Broad approach to compliance management**

Compliance management is (much) more than just meeting the requirements of laws and regulations. Organisations have to deal with many different types

## ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

*Debate amongst various politicians and legislators has increasingly focussed on ethical aspects of business conduct, meaning that directing the attitude of people and creating the right culture is more important*

of requirements from a variety of stakeholders (e.g. customers, sector organisations, etcetera), certificates and key standards and benchmarks that have been chosen on a voluntary basis and, *last but not least* their own company policies, rules and codes of business. In consequence, ethical business codes are taken more seriously nowadays as an indicator of good *corporate governance* and social responsibility. Management of all these different and mounting 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 organisation. 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 of both differences in approach and departmental objectives, management solutions applied to meet

these requirements will differ; there is therefore a potential overlap of concerns, or a risk that matters might fall between two stools. 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 the case of compliance with codes of conduct/ethics, debate amongst various politicians and legislators has increasingly focussed on ethical aspects of business conduct, meaning that directing the attitude of people and creating the right culture is more important. The proposed ISO standard will cover this broad scope of compliance management; an aspect where previous guidelines have perhaps been less attentive.

### **A flexible guideline**

ISO 19600 is developed as a *guideline* for compliance management and not as a *specification* that provides *requirements*. This was the preference of the majority of the ISO members that approved of the project. There are already enough certifiable management system standards for specific disciplines, that include

## ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

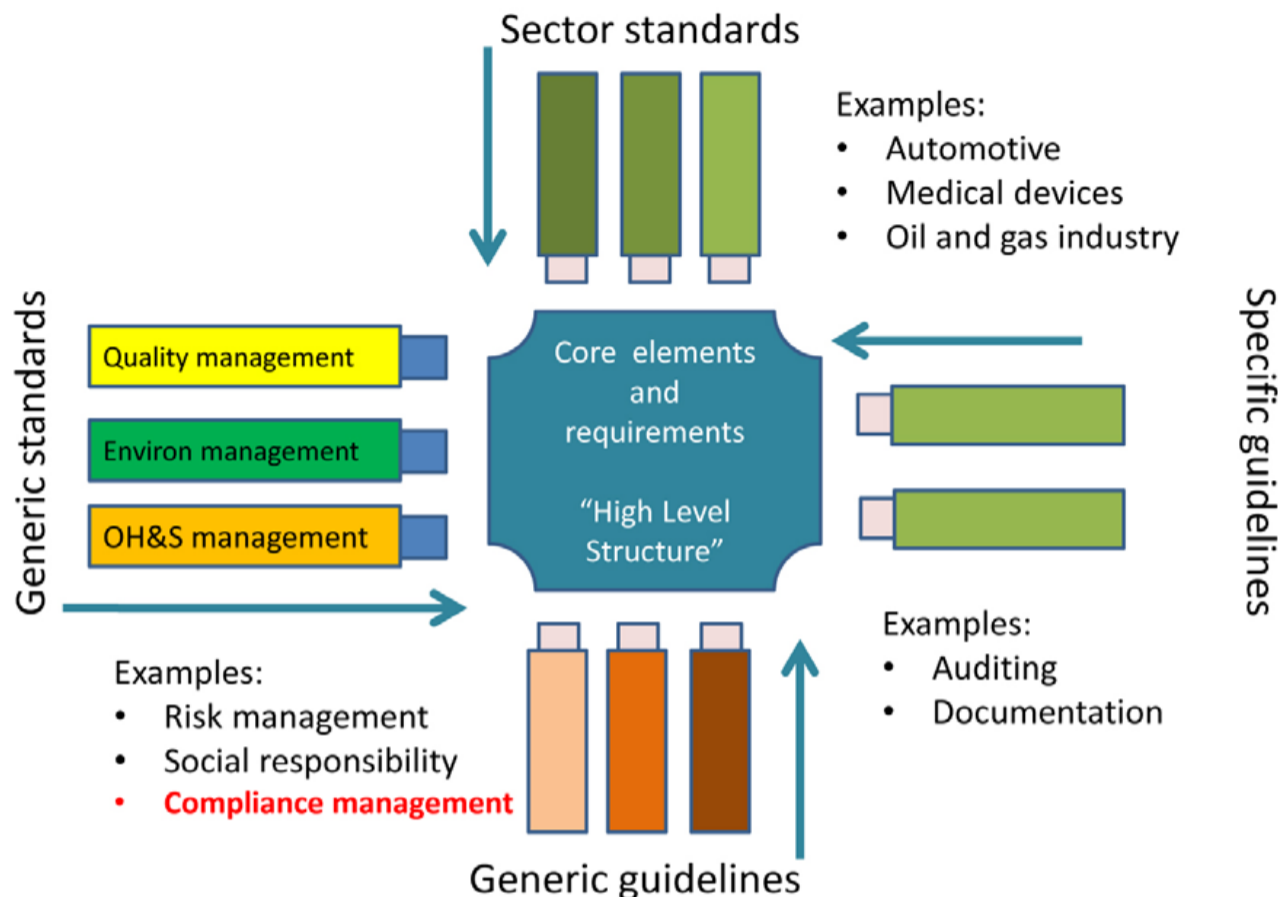


Figure 1 – Plug-in model for ISO management system standards

### ABOUT ISO

ISO (International Organisation for Standardization) is a global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented worldwide. ISO standards distil an international consensus from the broadest possible base of stakeholder groups. Expert input comes from those closest to the needs for the standards and also to the results of implementing them. In this way, although voluntary, ISO standards are widely respected and implemented by public and private sectors internationally.

ISO – a non-governmental organisation – is a network of the national standards bodies of some 160\* countries, one per country, from all regions

of the world, including developed, developing and transitional economies. Each ISO member is the principal standards organisation in its country. For example: NEN is the ISO member for the Netherlands and BSI the member for the United Kingdom. The members propose the new standards, participate in their development and provide support in collaboration with ISO Central Secretariat for more than 3,000 technical groups that actually develop the standards. ISO members appoint national delegations to standards committees. In all, there are some 50,000 experts contributing directly to the work of the organisation each year, plus an estimated 300,000 who follow the work and provide input to national “mirror” committees. When their work is published as an ISO International Standard, it may be translated and adopted as a national standard by the ISO members.

## ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

*Small and medium size companies should be able to evaluate and implement solutions appropriate to them, rather than be burdened to create such a management system which would lead to a considerable disadvantage*

compliance management as an important system element; e.g. ISO 14001 for environmental management or OHSAS 18001<sup>2</sup> for occupational health and safety management. ISO 19600 is intended to assist organisations in improving and broadening their existing approach to compliance management. Therefore it is helpful that ISO 19600 follows the so-called ‘*high level structure*’ for ISO management system standards. Consequently, the guideline can be applied as a ‘plug-in’ to adapt the overall management system of an organisation to manage compliance matters systematically as well (see figure 1).

Another reason why it is of importance to create a guideline instead of a certifiable management system is the fact that small and medium size companies should be able to evaluate and implement solutions appropriate to them, rather than be burdened to create such a management system which would lead to a considerable disadvantage for these companies. These businesses should embrace compliance and set up such a management system

that fits the needs and possibilities of the enterprise as such, and assist it in achieving the subjacent compliance goals.

### **Risk based approach**

As stated above, compliance management goes beyond the mere satisfaction of legal requirements. Compliance is also related to meeting the needs and expectations of a wide range of stakeholders. Therefore making sound choices and the setting of priorities is an important part of compliance management. ISO 19600 follows a risk-based approach to compliance management that is aligned with ISO 31000 (the ISO standard for risk management). This approach is visualized in figure 2. By analyzing the context and environment in which an organisation operates, its *compliance obligations* are determined. This means that the organisation has to decide upon which requirements, needs and expectations of its stakeholders are to be considered as obligations for the organisation and that will therefore be complied with. Such decisions will be based on a risk assessment that asks:

ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

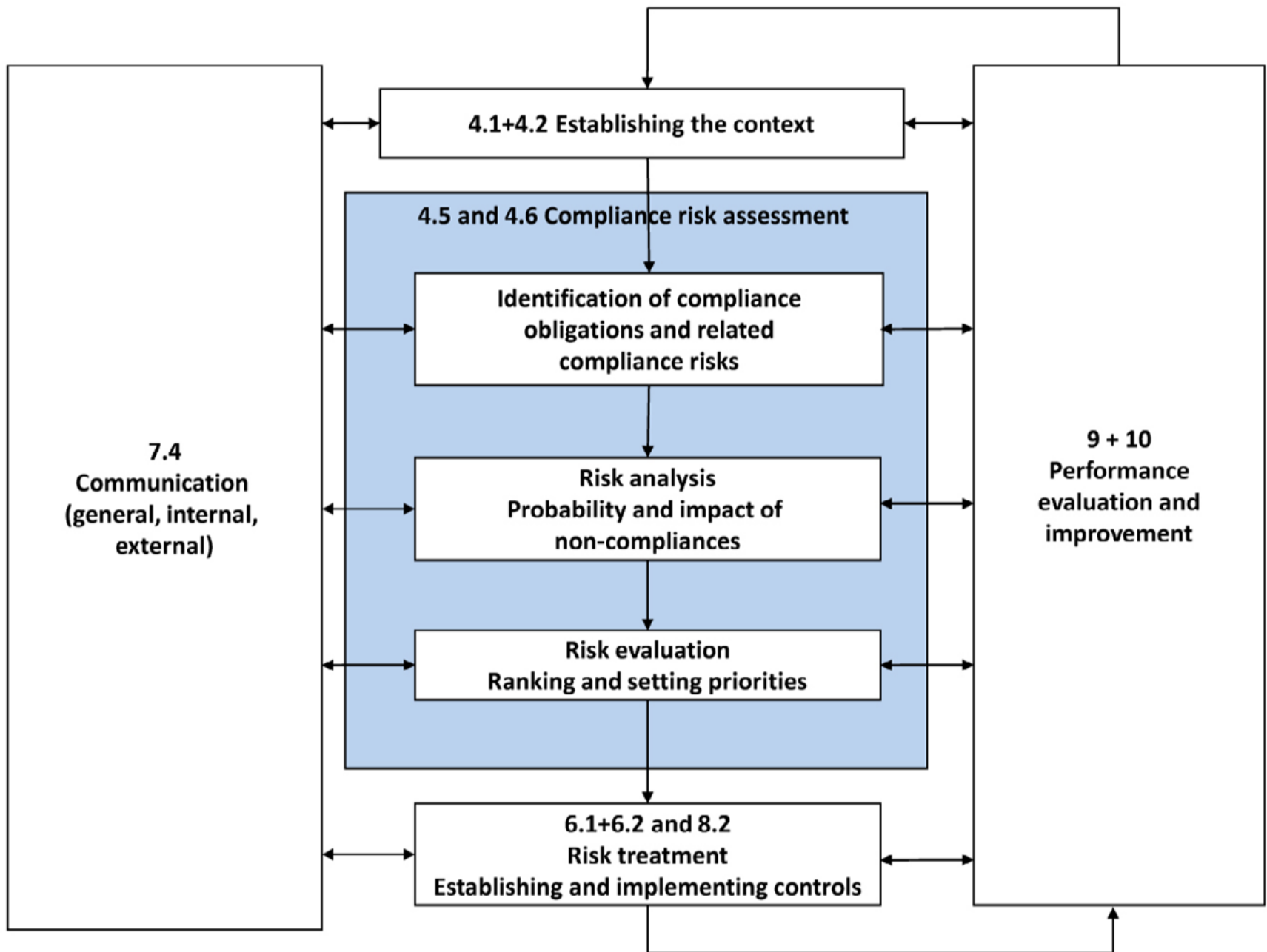


Figure 2 – Risk-based approach in ISO 19600 to compliance management according to ISO 31000 (numbers refer to clause number in ISO/DIS 19600)

What is the risk (threat or opportunity) if I do (not) adopt a stakeholder’s need as a compliance obligation? In case of legal requirements, the organisation has no choice: any socially responsible organisation has to comply with the law. However, on the basis of a risk assessment, priorities will be set to devote most management efforts and controls to those obligations with the largest compliance risks (expressed as

the likelihood of occurrence and the impact of the consequences of non-compliance). Based on the assessment of the compliance risk, mitigating measures (risk controls) are designed and implemented as well as methods and procedures to monitor and evaluate compliance and the effectiveness of the implemented controls. This risk-based approach assists organisations to provide focus for their compliance management.

## ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

*The standard devotes much attention to the roles and responsibilities of the governing body, top management, line management and employees of an organisation, as well as for the independence of the compliance officer*

In the box four key definitions from the *draft ISO 19600* are included. These show that the scope of compliance management covers both legal and voluntary obligations.

### **The compliance management system**

As stated, ISO 19600 follows the ‘High level structure’ (HLS) for ISO management

system standards. All the standard elements of a management system are adapted and supplemented for the subject of compliance (see the table overleaf). The standard devotes much attention to the roles and responsibilities of the governing body, top management, line management and employees of an organisation, as well as for the independence of the compliance officer (or more general:

---

### **KEY DEFINITIONS IN ISO/DIS 19600**

---

**COMPLIANCE:** meeting all the organisation’s *compliance obligations*

Note – compliance is made sustained by embedding it in the culture of an organisation and in the behaviour and attitude of people working for it

---

**COMPLIANCE OBLIGATION:** requirement that an organisation 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 organisational and industry standards and codes, contractual relationships, principles of good governance and community and ethical standards

---

**COMPLIANCE RISK:** effect of uncertainty on compliance objectives

Note – Compliance risk can be characterized by the likelihood of occurrence and the consequences of noncompliance with the organisation’s compliance obligations

---

**NONCOMPLIANCE:** non-fulfillment of a compliance obligation

Note – Noncompliance can be a single or multiple event and may or may not be the result of a system failure

---

ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

High Level Structure for ISO MSS	Guidance on compliance in ISO/DIS 19600
<b>Context of the organisation</b>	<ul style="list-style-type: none"> <li>■ Analysis of the environment in which the organisation operates (context, issues, stakeholders and their requirements, needs and expectations)</li> <li>■ Scope of the compliance management system</li> <li>■ Identification of compliance obligations</li> <li>■ Assessment of the compliance risks</li> </ul>
<b>Leadership</b>	<ul style="list-style-type: none"> <li>■ Policy, commitment, leading by example</li> <li>■ Roles, responsibilities and authorities with respect to compliance for the board, top and line management, employees and an independent compliance officer</li> </ul>
<b>Planning</b>	<ul style="list-style-type: none"> <li>■ Planning of measures to control compliance risks</li> <li>■ Establishing compliance objectives</li> </ul>
<b>Support</b>	<ul style="list-style-type: none"> <li>■ Awareness, competence and training in compliance</li> <li>■ Behaviour and culture</li> <li>■ Communication and documentation</li> </ul>
<b>Operation</b>	<ul style="list-style-type: none"> <li>■ Implementation of controls for compliance (technical, procedural, directing the attitude and behaviour of personnel)</li> </ul>
<b>Performance evaluation</b>	<ul style="list-style-type: none"> <li>■ Monitoring of compliance, application of indicators</li> <li>■ Analysis of information and reporting of results (internal and external)</li> <li>■ Internal Audit and Management Review</li> </ul>
<b>Improvement</b>	<ul style="list-style-type: none"> <li>■ Actions on non-compliance with requirements and escalation to higher management levels when necessary</li> <li>■ Corrective action</li> <li>■ Improvement activities</li> </ul>

**Table – Correspondence of the HLS system elements with specific guidance on compliance management**

the compliance function). The standard emphasizes that an exemplary role and commitment of management is essential to establish a culture where compliance is ‘the standard’ and employees at all levels and in all circumstances (can) show the right attitude and behaviour. The standard further recognizes that compliance lies in the end the result of the behaviour and actions of people, hence so-called soft controls become an

important part of any control measures. Monitoring of compliance and taking action on instances of non-compliance is described extensively, together with escalation expectations to appropriate management levels when necessitated by the seriousness of the instance of non-compliance. In figure 3, taken from ISO/DIS 19600, the relationship of the elements of compliance management according to the HLS is visualized.



ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

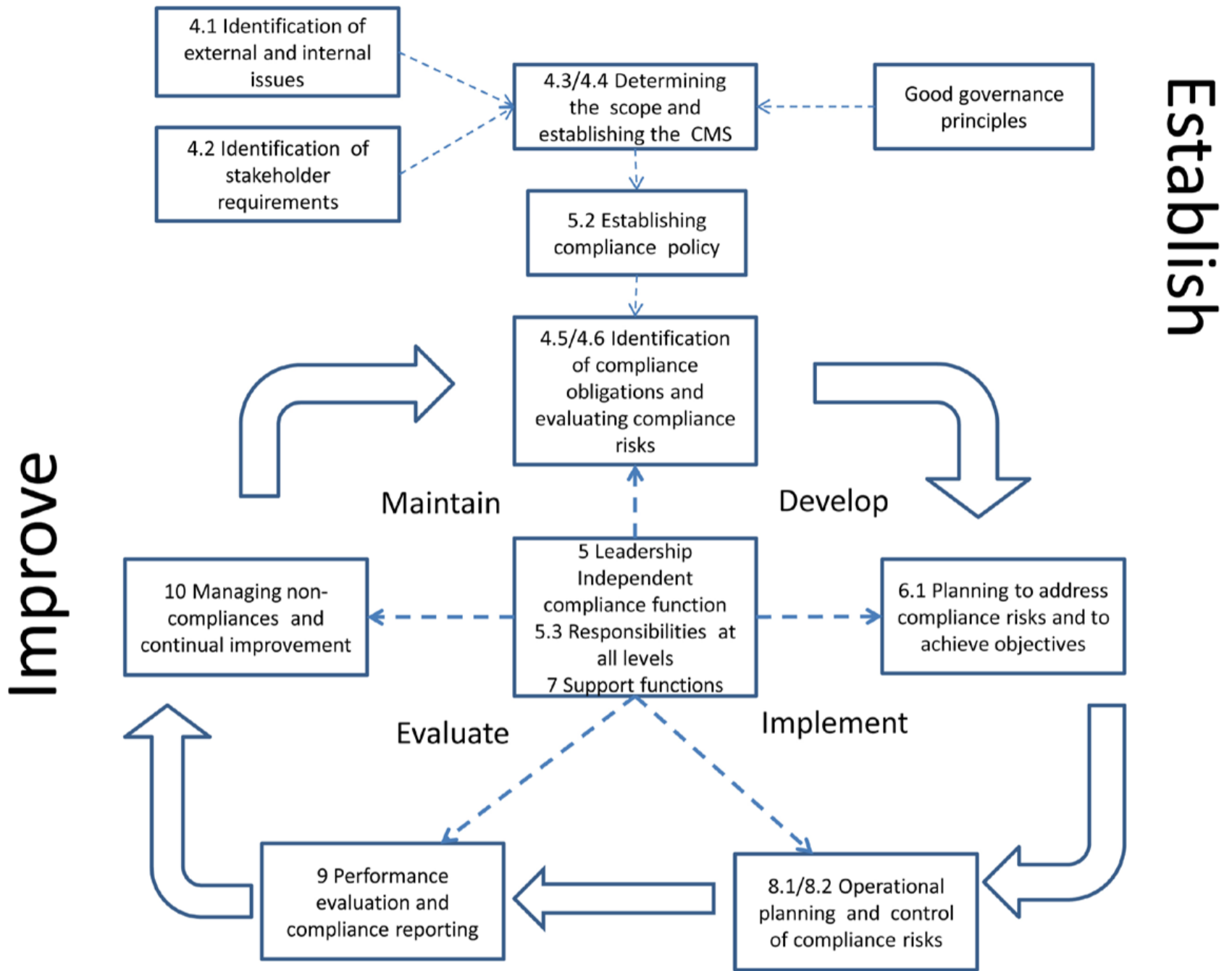


Figure 3 – relationship between the elements of compliance management according to ISO 19600 (numbers refer to clause number in ISO/DIS 19600)

**The significance of ISO 19600**

Compliance management is an important, at times critical, issue. Good conduct is after all at the foundation of a company’s ‘license to operate’. The growing number and complexity of (legal) requirements that have to be complied with demands a systematic and planned approach within an organisation. Government inspection

and supervising bodies can benefit when organisations accept their responsibility with respect to the implementation of, and compliance with laws and regulations more seriously. By evaluating the maturity of compliance management in organisations where they have to enforce the law, supervisory authorities can usefully adapt the quantitative and

## ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

*ISO 19600 is intended and designed to be used as the framework for a company wide compliance management programme with a good link to corporate policies and strategies*

qualitative approach to carrying out inspections and of maintaining oversight. By following guidelines that clarify what constitutes maturity, organisations can limit the disruption to business activities that normally accompany higher intensities of inspection visits. To support such approaches a generally accepted reference for ‘good compliance management’ is an important tool. ISO 19600 will provide that reference.

### **Integrated Compliance Management**

Compliance management is part of a range of other well-known management system standards, such as ISO 14001 and OHSAS 18001. In terms of structure and content, ISO 19600 is aligned with the next generation of these management system standards and is therefore very suitable to enhance the compliance component of environmental and occupational health and safety management. ISO 19600 also provides a good interpretation of the basic compliance related requirements that are part of the core requirements of the High Level Structure (“HLS”) (see figure 1). Therefore ISO 19600 is intended and designed to be used

as the framework for a company wide compliance management programme with a good link to corporate policies and strategies, as well as with specific operational management activities of other risk disciplines.

In the post financial crisis era, there has been an increasing emphasis of the vital role and importance of effective corporate Governance, Risk and Compliance management (“GRC”) as the essence for a successful and socially responsible business. For risk management the global reference is ISO 31000, for corporate governance, reference can be made to the ISO HLS and core requirements for management systems. In early 2015, ISO 19600 will complement these existing tools to become the reference document for compliance management. Together these ISO standards will provide the tools for managing an organisation in a responsible way. Transparent application of risk and compliance management standards as an integrated part of corporate governance offers a good means by which to counteract the increasing burden of rules and regulations, and to find a new balance between the exercise

## ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

*In a world where social responsibility extends to the business practices of all associated partners and service providers, a standard defining accepted business compliance arrangements will have a significant impact*

and adherence by companies of their own (social) responsibilities on one hand, and the effective pursuit of oversight responsibilities of regulatory bodies and governments on the other.

### **Next steps**

ISO member bodies are able to vote and provide comments on the *Draft International Standard* until 22 April 2014. During the next meeting of ISO/PC 271 in July 2014 in Vienna, the results of the voting and comments received will be reviewed, and the text of the next draft version prepared. Assuming that the vote will be positive, the next draft of ISO 19600 will be issued as a *Final Draft International Standard* for a final ballot amongst the ISO members. Then the standard may be published by ISO at the beginning of 2015

### **Comments on the ISO Standard**

Until the 21<sup>st</sup> of April 2014 comments will be collected through the national standardization committees. It is of particular importance that the global compliance community is aware of the creation of the ISO standard/guideline on compliance management, due to

the influence the standard will have on companies assessing the compliance system of business partners in the future. Even at this late stage, compliance experts need to grasp the opportunity to ascertain that the ISO standard is not only theoretically correct, but also practically effective. Although the ISO compliance guideline will not lead to certification, companies may very well decide to use the standard to assess potential business partners, agencies, distributors and outsourcing contracts included, verifying that they measure up to the ISO guideline; alternatively B2B clients, suppliers, distributors and other business partners may use the standard to benchmark alignment and the maturity of compliance management at your organisation. Whichever what way ... in a world where social responsibility extends to the business practices of all associated partners and service providers, a standard defining accepted business compliance arrangements will have a significant impact.

The ISO guideline on compliance management systems is intended for all kinds of companies and a wide diversity of business activities. The standard applies

### ISO 19600: THE DEVELOPMENT OF A GLOBAL STANDARD ON COMPLIANCE MANAGEMENT

to financial institutions as well as non-financial companies (industrial, services, etc.). For unregulated companies, the choice of a guideline over a standard is preferable, due to the fact that small and medium companies may not be able to set up quite as elaborate a system as larger companies might. As a result, the use of a standard would lead to quite a disadvantage for smaller businesses. The guideline offers smaller businesses insight in how to best be in control of the compliance requirements, but leaves them the possibility to set up a compliance system that is fit for purpose. A review and impact analysis of ISO 19600 on your organisation might seem a very timely act indeed.

#### **More information**

More information on this subject can be provided by Dick Hortensius, +31 15 2 690 115, e-mail: [dick.hortensius@nen.nl](mailto:dick.hortensius@nen.nl)

#### **Post Script**

The Draft International Standard ISO/DIS 19600 is published for voting and comments with a deadline ending 21 April 2014. Persons that would like to provide feedback on ISO/DIS 19600 should contact the ISO member body in their country.<sup>3</sup> Some countries already have joined the ISO Project Committee on the ISO Compliance Management System, but they will also appreciate the extra input.<sup>4</sup> ■

---

<sup>3</sup> [http://www.iso.org/iso/home/about/iso\\_members.htm](http://www.iso.org/iso/home/about/iso_members.htm)

<sup>4</sup> Argentina, Australia, Austria, Canada, China, Denmark, France, Germany, Malaysia, Netherlands, Singapore, Spain and Switzerland.