INTERNATIONAL STANDARD

ISO 19600

First edition
2014-12-15

Compliance management systems — Guidelines

Systèmes de management de la conformité — Lignes directrices

Reference number
ISO 19600:2014(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is Project Committee ISO/PC 271, *Compliance management systems*.

Introduction

Organizations that aim to be successful in the long term need to maintain a culture of integrity and compliance, and to consider the needs and expectations of stakeholders. Integrity and compliance are therefore not only the basis, but also an opportunity, for a successful and sustainable organization.

Compliance is an outcome of an organization meeting its obligations, and is made sustainable by embedding it in the culture of the organization and in the behaviour and attitude of people working for it. While maintaining its independence, it is preferable if compliance management is integrated with the organization's financial, risk, quality, environmental and health and safety management processes and its operational requirements and procedures.

An effective, organization-wide compliance management system enables an organization to demonstrate its commitment to compliance with relevant laws, including legislative requirements, industry codes and organizational standards, as well as standards of good corporate governance, best practices, ethics and community expectations.

An organization's approach to compliance is ideally shaped by the leadership applying core values and generally accepted corporate governance, ethical and community standards. Embedding compliance in the behaviour of the people working for an organization depends above all on leadership at all levels and clear values of an organization, as well as an acknowledgement and implementation of measures to promote compliant behaviour. If this is not the case at all levels of an organization, there is a risk of noncompliance.

In a number of jurisdictions, the courts have considered an organization's commitment to compliance through its compliance management system when determining the appropriate penalty to be imposed for contraventions of relevant laws. Therefore, regulatory and judicial bodies can also benefit from this International Standard as a benchmark.

Organizations are increasingly convinced that by applying binding values and appropriate compliance management, they can safeguard their integrity and avoid or minimize noncompliance with the law. Integrity and effective compliance are therefore key elements of good, diligent management. Compliance also contributes to the socially responsible behaviour of organizations.

This International Standard does not specify requirements, but provides guidance on compliance management systems and recommended practices. The guidance in this International Standard is intended to be adaptable, and the use of this guidance can differ depending on the size and level of maturity of an organization's compliance management system and on the context, nature and complexity of the organization's activities, including its compliance policy and objectives.

The flowchart in Figure 1 is consistent with other management systems and is based on the continual improvement principle ("Plan-Do-Check-Act").

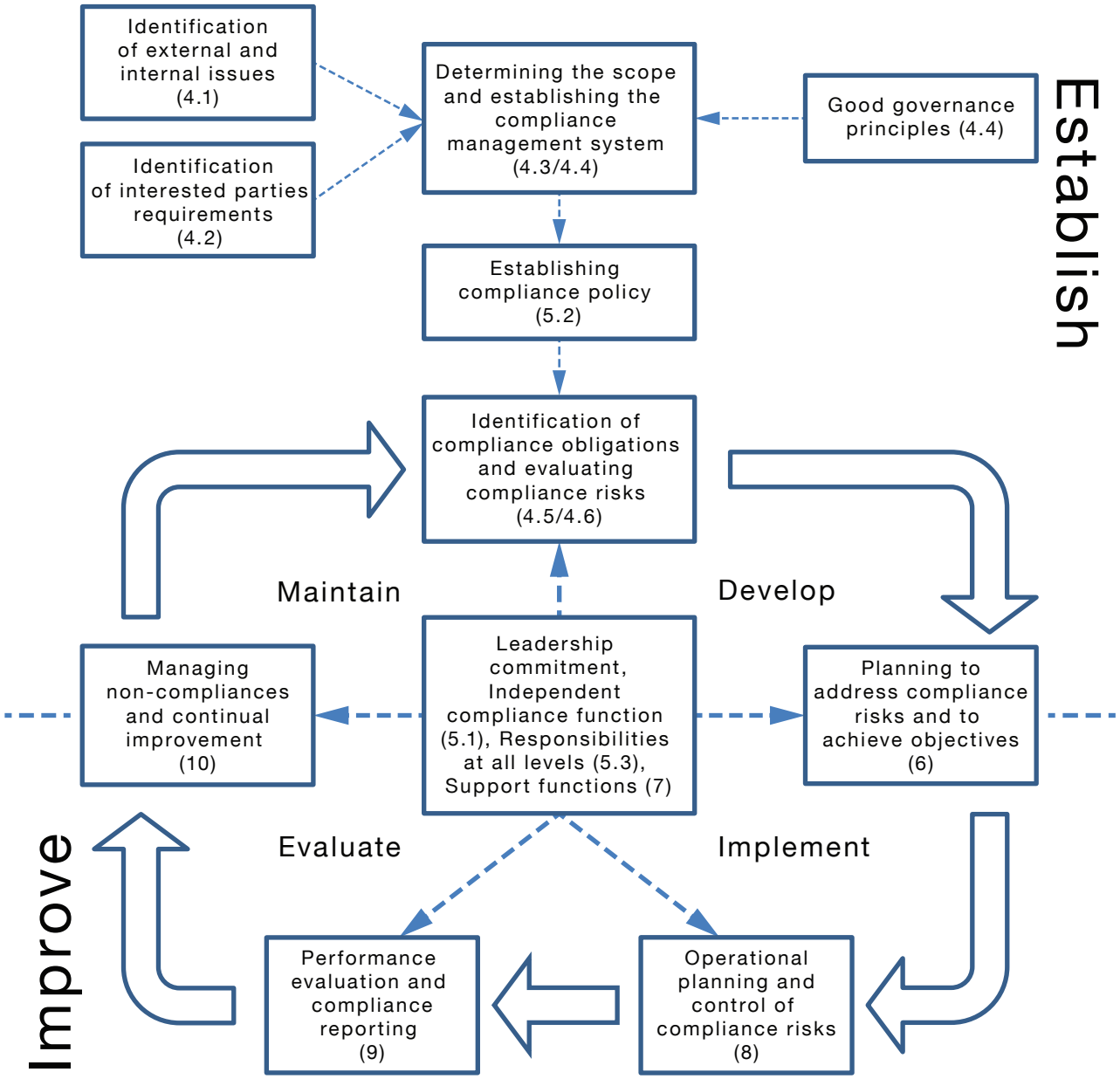

Figure 1 — Flowchart of a compliance management system

This International Standard has adopted the "high-level structure" (i.e. clause sequence, common text and common terminology) developed by ISO to improve alignment among its International Standards for management systems. In addition to its generic guidance on a compliance management system, this International Standard also provides a framework to assist in the implementation of specific compliance-related requirements in any management system.

Organizations that have not adopted management system standards or a compliance management framework can easily adopt this International Standard as stand-alone guidance within their organization.

This International Standard is suitable to enhance the compliance-related requirements in other management systems and to assist an organization in improving the overall management of all its compliance obligations.

This International Standard can be combined with existing management system standards (e.g. ISO 9001, ISO 14001, ISO 22000) and generic guidelines (e.g. ISO 31000, ISO 26000).

Compliance management systems — Guidelines

1 Scope

This International Standard provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization.

The guidelines on compliance management systems are applicable to all types of organizations. The extent of the application of these guidelines depends on the size, structure, nature and complexity of the organization. This International Standard is based on the principles of good governance, proportionality, transparency and sustainability.

2 Normative references

There are no normative references.

3 Terms and definition

For the purpose of this document, the following terms and definitions apply.

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.9)

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

3.2
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.1) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

3.3
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.7) covers only part of an organization then top management refers to those who direct and control that part of the organization.

3.4
governing body
person or group of people that governs an *organization* (3.1), sets directions and holds *top management* (3.3) to account

3.5
employee
individual in a relationship recognized as an employment relationship in national law or practice

3.6
compliance function
person(s) with responsibility for *compliance* (3.17) management

Note 1 to entry: Preferably one individual will be assigned overall responsibility for *compliance* (3.17) management

3.7
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.8) and *objectives* (3.9) and *processes* (3.10) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.8
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.7)

3.9
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical and/or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.10)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a compliance objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of compliance management systems, compliance objectives are set by the organization, consistent with the compliance policy, to achieve specific results.

3.10
process
set of interrelated or interacting activities which transforms inputs into outputs

3.11
risk
effect of uncertainty on *objectives* (3.9)

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

3.12
compliance risk
effect of uncertainty on compliance *objectives* (3.9)

Note 1 to entry: Compliance risk can be characterized by the likelihood of occurrence and the consequences of *noncompliance* (3.18) with the organization's *compliance obligations* (3.16).

3.13
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in documented information.

3.14
compliance requirement
requirement (3.13) that an *organization* (3.1) has to comply with

3.15
compliance commitment
requirement (3.13) that an *organization* (3.1) chooses to comply with

3.16
compliance obligation
compliance requirement (3.14) or *compliance commitment* (3.15)

3.17
compliance
meeting all the organization's *compliance obligations* (3.16)

Note 1 to entry: Compliance is made sustained by embedding it in the culture of an *organization* (3.1) and in the behaviour and attitude of people working for it.

3.18
noncompliance
non-fulfilment of a *compliance obligation* (3.16)

Note 1 to entry: Noncompliance can be a single or a multiple event and may or may not be the result of a *nonconformity* (3.33).

3.19
compliance culture
values, ethics and beliefs that exist throughout an *organization* (3.1) and interact with the organization's structures and control systems to produce behavioural norms that are conducive to *compliance* (3.17) outcomes

3.20
code
statement of practice developed internally or by an international, national or industry body or other *organization* (3.1)

Note 1 to entry: The code may be mandatory or voluntary.

3.21
organizational and industry standards
documented *codes* (3.20), good practices, charters , technical and industry standards deemed by an *organization* (3.1) to be relevant

3.22
regulatory authority
organization (3.1) responsible for regulating or enforcing *compliance* (3.17) with legislative and other *requirements* (3.13)

3.23
competence
ability to apply knowledge and skills to achieve intended results

3.24
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.7), including related *processes* (3.10);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.25
procedure
specified way to carry out an activity or *process* (3.10)

3.26
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.10), products (including services), systems or *organizations* (3.1).

3.27
continual improvement
recurring activity or *process* (3.10) to enhance *performance* (3.26)

3.28
outsource (verb)
make an arrangement where an external *organization* (3.1) performs part of an organization's function or *process* (3.10)

Note 1 to entry: An external organization is outside the *management system* (3.7), although the outsourced function or process is within the scope.

3.29
monitoring
determining the status of a system, a *process* (3.10) or an activity

Note 1 to entry: To determine the status there may be a need to check, supervise or critically observe.

Note 2 to entry: Monitoring is not a once-only activity, but a process of regularly or continuously observing a situation.

3.30
measurement
process (3.10) to determine a value

3.31
audit
systematic, independent and documented *process* (3.10) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

Note 3 to entry: Independence can be demonstrated by the freedom from responsibility for the activity being audited or freedom from bias and conflict of interest.

3.32
conformity
fulfilment of a management system *requirement* (3.13)

3.33
nonconformity
non-fulfilment of a management system *requirement* (3.13)

Note 1 to entry: A nonconformity is not necessarily a *noncompliance* (3.18).

3.34
correction
action to eliminate a detected *nonconformity* (3.33) or a *noncompliance* (3.18)

3.35
corrective action
action to eliminate the cause of a *nonconformity* (3.33) or a *noncompliance* (3.18) and to prevent recurrence

4 Context of the organization

4.1 Understanding the organization and its context

The organization should determine external and internal issues, such as those related to compliance risks, that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its compliance management system. In doing so, the organization should consider a broad range of external and internal aspects, such as the regulatory, social and cultural contexts, the economic situation and the internal policies, procedures, processes and resources.

4.2 Understanding the needs and expectations of interested parties

The organization should determine:

— the interested parties that are relevant to the compliance management system;

— the requirements of these interested parties.

4.3 Determining the scope of the compliance management system

The organization should determine the boundaries and applicability of the compliance management system to establish its scope.

NOTE The scope of the compliance management system is intended to clarify the geographical and/or organizational boundaries to which the compliance management system will apply, especially if the organization is a part of a larger organization at a given location.

When determining this scope, the organization should consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2 and 4.5.1.

The scope should be readily available as documented information.

4.4 Compliance management system and principles of good governance

The organization should establish, develop, implement, evaluate, maintain and continually improve a compliance management system, including the processes needed and their interactions, in accordance with this International Standard, taking into consideration the following governance principles:

— direct access of the compliance function to the governing body;

— independence of the compliance function;

— appropriate authority and adequate resources allocated to the compliance function.

The compliance management system should reflect the organization's values, objectives, strategy and compliance risks.

4.5 Compliance obligations

4.5.1 Identification of compliance obligations

The organization should systematically identify its compliance obligations and their implications for its activities, products and services. The organization should take these obligations into account in establishing, developing, implementing, evaluating, maintaining and improving its compliance management system.

The organization should document its compliance obligations in a manner that is appropriate to its size, complexity, structure and operations.

Sources of compliance obligations should include compliance requirements and can include compliance commitments.

EXAMPLE 1 Examples of compliance requirements include:

— laws and regulations;

— permits, licences or other forms of authorization;

— orders, rules or guidance issued by regulatory agencies;

— judgments of courts or administrative tribunals;

— treaties, conventions and protocols.

EXAMPLE 2 Examples of compliance commitments include:

— agreements with community groups or non-governmental organizations;

— agreements with public authorities and customers;

— organizational requirements, such as policies and procedures;

— voluntary principles or codes of practice;

— voluntary labelling or environmental commitments;

— obligations arising under contractual arrangements with the organization;

— relevant organizational and industry standards.

4.5.2 Maintenance of compliance obligations

Organizations should have processes in place to identify new and changed laws, regulations, codes and other compliance obligations to ensure on-going compliance. Organizations should have processes to

evaluate the impact of the identified changes and implement any changes in the management of the compliance obligations.

EXAMPLE Examples of processes to obtain information on changes to laws and other compliance obligations include:

— being on the mailing lists of relevant regulators;

— membership of professional groups;

— subscribing to relevant information services;

— attending industry forums and seminars;

— monitoring the websites of regulators;

— meeting with regulators;

— arrangements with legal advisors;

— monitoring the sources of the compliance obligations (e.g. regulatory pronouncements and court decisions).

4.6 Identification, analysis and evaluation of compliance risks

The organization should identify and evaluate its compliance risks. This evaluation can be based on a formal compliance risk assessment or conducted via alternative approaches. Compliance risk assessment constitutes the basis for the implementation of the compliance management system and the planned allocation of appropriate and adequate resources and processes to manage identified compliance risks.

The organization should identify compliance risks by relating its compliance obligations to its activities, products, services and relevant aspects of its operations in order to identify situations where noncompliance can occur. The organization should identify the causes for and consequences of noncompliance.

The organization should analyse compliance risks by considering causes and sources of noncompliance and the severity of their consequences, as well as the likelihood that noncompliance and associated consequences can occur. Consequences can include, for example, personal and environmental harm, economic loss, reputational harm and administrative liability.

Risk evaluation involves comparing the level of compliance risk found during the analysis process with the level of compliance risk the organization is able and willing to accept. Based on this comparison, priorities can be set as a basis for determining the need for implementing controls and the extent of these controls (see 6.1).

The compliance risks should be reassessed periodically and whenever there are:

— new or changed activities, products or services;

— changes to the structure or strategy of the organization;

— significant external changes, such as financial-economic circumstances, market conditions, liabilities and client relationships;

— changes to compliance obligations (see 4.5);

— noncompliance(s).

NOTE 1 The extent and level of detail of the compliance risk assessment are dependent on the risk situation, context, size and objectives of the organization and can vary for specific sub-areas (e.g. environment, financial, social).

NOTE 2 The risk-based approach to compliance management does not mean that for low compliance risk situations, noncompliance is accepted by the organization. It assists organizations in focussing primary attention and resources on higher risks as a priority, and ultimately will cover all compliance risks. All identified compliance risks/situations are subject to monitoring, correction and corrective action.

NOTE 3 ISO 31000 provides detailed guidance on risk assessment.

5 Leadership

5.1 Leadership and commitment

The governing body and top management should demonstrate leadership and commitment with respect to the compliance management system by:

a) establishing and upholding the core values of the organization;

b) ensuring that the compliance policy and compliance objectives are established and are consistent with the values, objectives and strategic direction of the organization (see 6.2);

c) ensuring that policies, procedures and processes are developed and implemented to achieve compliance objectives;

d) ensuring that the resources needed for the compliance management system are available, allocated and assigned;

e) ensuring the integration of the compliance management system requirements into the organization's business processes;

f) communicating the importance of an effective compliance management system and the importance of conforming to the compliance management system requirements;

g) directing and supporting persons to contribute to the effectiveness of the compliance management system;

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of compliance responsibility;

i) ensuring alignment between operational targets and compliance obligations;

j) establishing and maintaining accountability mechanisms, including timely reporting on compliance matters, including noncompliance;

k) ensuring that the compliance management system achieves its intended outcome(s);

l) promoting continual improvement.

EXAMPLE Effective compliance requires an active commitment from the governing body and top management that permeates the whole organization. The level of commitment is indicated by the degree to which:

— the governing body and all levels of management actively demonstrate commitment to establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system through their actions and decisions;

— the compliance policy is formally approved by the governing body;

— top management takes responsibility for ensuring that the commitment to compliance of the organization is fully realized;

— all levels of management consistently convey a clear message (demonstrated by words and actions) to employees that the organization will meet its compliance obligations;

— the commitment to compliance is communicated widely in clear and convincing statements supported by action;

— the compliance function is given a level of authority which reflects the importance of effective compliance and has direct access to the governing body;

— resources are allocated to establishing, developing, implementing, evaluating, maintaining and improving a robust compliance culture though awareness-raising activities and training;

— policies, procedures and processes reflect not just the legal requirements, but also voluntary codes and the organization's core values;

— the organization assigns and requires accountability for compliance to management across all levels of the organization;

— regular review of the compliance management system is required;

— compliance performance of the organization is continually improved;

— corrective action is taken.

5.2 Compliance policy

5.2.1 General

The governing body and top management, preferably in consultation with employees, should establish a compliance policy that

— is appropriate to the purpose of the organization;

— provides a framework for setting compliance objectives;

— includes a commitment to satisfy applicable requirements;

— includes a commitment to continual improvement of the compliance management system.

The compliance policy should articulate:

— the scope of the compliance management system;

— the application and context of the system in relation to the size, nature and complexity of the organization and its operating environment;

— the extent to which compliance will be integrated with other functions, such as governance, risk, audit and legal;

— the degree to which compliance will be embedded into operational policies, procedures and processes;

— the degree of independence and autonomy of the compliance function;

— the responsibility for managing and reporting compliance issues;

— the principles on which relationships with internal and external stakeholders will be managed;

— the required standard of conduct and accountability;

— the consequences of noncompliance.

The compliance policy should:

— be available as documented information;

— be written in plain language so that all employees can easily understand the principles and intent;

— be translated into other languages if necessary;

— be communicated clearly within the organization and be made readily available to all employees;

— be available to interested parties, as appropriate;

— be updated, as required, to ensure it remains relevant.

The compliance policy should be established in alignment with the organization's values, objectives and strategy, and should be endorsed by the governing body.

The compliance policy establishes the overarching principles and commitment to action for an organization to achieving compliance. It sets the level of responsibility and performance required and sets expectations to which actions will be assessed. The policy should be appropriate to the organization's compliance obligations that arise from its activities.

The compliance policy should not be a stand-alone document but should be supported by other documents, including operational policies, procedures and processes.

5.2.2 Development

In developing the compliance policy, consideration should be given to:

a) specific international, regional, or local obligations;

b) the organization's strategy, objectives and values;

c) the organization's structure and governance framework;

d) the nature and level of risk associated with noncompliance;

e) other internal policies, standards and codes.

5.3 Organizational roles, responsibilities and authorities

5.3.1 General

Top management should ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

The governing body and top management should assign the responsibility and authority to the compliance function for:

a) ensuring that the compliance management system is consistent with this International Standard;

b) reporting on the performance of the compliance management system to the governing body and top management.

NOTE The specific duties of the compliance function do not relieve other employees of responsibilities for reporting on compliance that might exist.

5.3.2 Assigning responsibility for compliance in the organization

The active involvement of, and supervision by, governing body and top management is an integral part of an effective compliance management system. This helps ensure that employees fully understand the organization's policy and operational procedures and how these apply to their jobs, and that they carry out compliance obligations effectively.

For a compliance management system to be effective the governing body and top management need to lead by example, by adhering to and actively supporting compliance and the compliance management system.

Many organizations have a dedicated person (e.g. a compliance officer) responsible for day-to-day compliance management, and some have a cross-functional compliance committee to coordinate compliance across the organization.

Some organizations – depending on their size –also have someone who has overall responsibility for compliance management, although this may be in addition to other roles or functions, including existing committees, organizational unit(s), or outsource elements to compliance experts.

This should not be seen as absolving other levels of management of their compliance responsibilities, as all managers have a role to play with respect to the compliance management system. It is therefore important that their respective responsibilities are clearly set out and included in their job descriptions.

Compliance responsibilities of managers will, by necessity, vary according to levels of authority, influence and other factors, such as the nature and size of the organization. However, some responsibilities are likely to be common across a variety of organizations.

NOTE This International Standard does not distinguish between the concept of responsibility and that of accountability. Accountability is implicit in the use of the term "responsibility".

5.3.3 Governing body and top management role and responsibility

The governing body and top management should:

a) establish a compliance policy in accordance with 5.2.2;

b) ensure that the commitment to compliance is maintained and that noncompliance and noncompliant behaviour are dealt with appropriately;

c) include compliance responsibilities in position statements of top managers;

d) appoint or nominate a compliance function with:

   1) authority and responsibility for the design, consistency and integrity of the compliance management system;

   2) clear and unambiguous support from and direct access to the governing body and top management;

   3) access to:

      — senior decision-makers and the opportunity to contribute early in the decision-making processes;

      — all levels of the organization:

      — all documented information and data needed to perform the compliance tasks;

      — expert advice on relevant laws, regulations, codes and organizational standards;

   4) the authority and capacity to execute countervailing power, by showing any consequences for compliance in relevant decision-making processes;

e) ensure that the compliance function has authority to act independently and is not compromised by conflicting priorities, particularly where compliance is embedded in the business.

Top management should:

— allocate adequate and appropriate resources to establish, develop, implement, evaluate, maintain and improve the compliance management system and performance outcomes;

— ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization;

— ensure that effective and timely systems of reporting are in place;

— be measured against compliance key performance measures or outcomes;

— assign responsibility for reporting on the performance of the compliance management system to governing body and top management.

5.3.4 Compliance function

Not all organizations will create a discrete compliance function, some may assign this function to an existing position.

The compliance function, working together with management, should be responsible for:

a) identifying compliance obligations with the support of relevant resources and translating those obligations into actionable policies , procedures and processes;

b) integrating compliance obligations into existing policies, procedures and processes ;

c) providing or organizing on-going training support for employees to ensure that all relevant employees are trained on a regular basis;

d) promoting the inclusion of compliance responsibilities into job descriptions and employee performance management processes;

e) setting in place a compliance reporting and documenting system;

f) developing and implementing processes for managing information, such as complaints and/or feedback by means of hotlines, a whistle-blowing system and other mechanisms;

g) establishing compliance performance indicators and monitoring and measuring compliance performance;

h) analysing performance to identify the need for corrective action;

i) identifying compliance risks and managing those compliance risks relating to third parties, such as suppliers, agents, distributors, consultants and contractors;

j) ensuring the compliance management system is reviewed at planned intervals;

k) ensuring there is access to appropriate professional advice in the establishment and implementation and maintaining of the compliance management system;

l) providing employees with access to resources on compliance procedures and references;

m) providing objective advice to the organization on compliance-related matters.

NOTE Guidelines for complaints handling are provided in ISO 10002.

In allocating responsibility for compliance management, consideration should be given to ensuring that the compliance function has no conflict of interest and has demonstrated:

— integrity and commitment to compliance;

— effective communication and influencing skills;

— an ability and standing to command acceptance of advice and guidance;

— relevant competence.

5.3.5 Management responsibilities

Management should be responsible for compliance within its area of responsibility. This includes:

a) cooperating with and supporting the compliance function and encouraging employees to do the same;

b) personally complying and being seen to comply with policies, procedures and processes and attending and supporting compliance training activities;

c) identifying and communicating compliance risks in their operations;

d) actively undertaking and encouraging mentoring, coaching and supervising employees to promote compliant behaviour;

e) encouraging employees to raise compliance concerns;

f) actively participating in the management and resolution of compliance-related incidents and issues;

g) developing employee awareness of compliance obligations and directing them to meet training and competence requirements;

h) ensuring compliance is factored into job descriptions;

i) integrating compliance performance into employee performance appraisals (e.g. KPIs, targets and promotion criteria);

j) integrating compliance obligations into existing business practices and procedures in their areas of responsibility;

k) in conjunction with the compliance function, ensuring that once the need for corrective action is identified, it is implemented;

l) overseeing outsourcing arrangements to ensure they take account of compliance obligations.

5.3.6 Employee responsibility

All employees, including managers, should:

a) adhere to the compliance obligations of the organization that are relevant to their position and duties;

b) participate in training in accordance with the compliance management system;

c) use available compliance resources as a part of the compliance management system;

d) report compliance concerns, issues and failures.

6 Planning

6.1 Actions to address compliance risks

When planning for the compliance management system, the organization should consider the issues referred to in 4.1, the requirements referred to in 4.2, the principles of good governance referred to in 4.4, the compliance obligations identified in 4.5 and the results of the compliance risk assessment referred to in 4.6 to determine the compliance risks that need to be addressed to:

— assure the compliance management system can achieve its intended outcome(s);

— prevent, detect and reduce undesired effects;

— achieve continual improvement.

The organization should plan:

a) actions to address these compliance risks and

b) how to:

  — integrate and implement the actions into its compliance management system processes;

  — evaluate the effectiveness of these actions.

The organization should retain documented information on the compliance risks and on the planned actions to address them.

6.2 Compliance objectives and planning to achieve them

The organization should establish its compliance management system objectives at relevant functions and levels.

The compliance objectives should:

a) be consistent with the compliance policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated;

f) be updated and/or revised as appropriate.

When planning how to achieve its compliance objectives, the organization should determine:

— what will be done;

— what resources will be required;

— who will be responsible;

— when it will be completed;

— how the results will be evaluated, e.g. pursuant to identified compliance key performance measures and outcomes.

The organization should retain documented information on the compliance objectives and on the planned actions to achieve them.

7 Support

7.1 Resources

The organization should determine and provide the resources needed for the establishment, development, implementation, evaluation, maintenance and continual improvement of the compliance management system appropriate to its size, complexity, structure and operations.

Top management and all other levels of management should ensure that the necessary resources are deployed effectively to ensure that the compliance management system meets its objectives, and that compliance is achieved.

Resources include financial and human resources, as well as access to external advice and specialized skills, organizational infrastructure, contemporary reference material on compliance management and legal obligations, professional development and technology.

7.2 Competence and training

7.2.1 Competence

The organization should:

a) determine the necessary competence of employee(s) doing work under its control that affects its compliance management system performance;

b) ensure that these employees are competent on the basis of appropriate education, training and/or work experience;

c) where applicable, take actions to acquire the necessary competence and evaluate the effectiveness of the actions taken;

d) retain appropriate documented information, including evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the reassignment of employees; or the hiring or contracting of competent persons.

7.2.2 Training

The governing body, management and all employees have compliance obligations should be competent to discharge these effectively. The attainment of competence can be achieved in many ways, including skills and knowledge required through education, training or work experience.

The objective of a training program is to ensure that all employees are competent to fulfil their job role in a manner that is consistent with the organization's compliance culture and its commitment to compliance.

Properly designed and executed training can provide an effective way for employees to communicate previously unidentified compliance risks.

Education and training of employees should be:

a) tailored to the obligations and compliance risks related to the roles and responsibilities of the employee;

b) where appropriate, based on an assessment of gaps in employee knowledge and competence;

c) undertaken at commencement with the organization and be on-going ;

d) aligned to the corporate training program and be incorporated into annual training plans;

e) practical and readily understood by employees;

f) relevant to the day-to-day work of employees and illustrative of the industry, organization or sector concerned;

g) sufficiently flexible to account for a range of techniques to accommodate the differing needs of organizations and employees;

NOTE Interactive training might be the best form of training, if noncompliance could result in serious consequences.

h) assessed for effectiveness;

i) updated as required;

j) recorded and retained.

Compliance retraining should be considered whenever there is a:

— change of position or responsibilities;

— changes in internal, policies, procedures and processes;

— changes in organization structure;

— change in the compliance obligations, especially in legal or interested parties requirements;

— change in activities, products or services;

— issues arising from monitoring, auditing, reviews, complaints and noncompliance, including stakeholder feedback.

7.3 Awareness

7.3.1 General

Persons doing work under the organization's control should be aware of:

a) the compliance policy;

b) their role and contribution to the effectiveness of the compliance management system, including the benefits of improved compliance management system performance;

c) the implications of not conforming with the compliance management system requirements.

7.3.2 Behaviour

7.3.2.1 General

Behaviour that creates and supports compliance should be encouraged and behaviour that compromises compliance should not be tolerated.

7.3.2.2 Role of top management in encouraging compliance

Top management has a key responsibility for:

a) aligning the organization's commitment to compliance to its values, objectives and strategy in order to position compliance appropriately;

b) communicating its commitment to compliance in order to build awareness and motivate employees to embrace the compliance management system;

c) encouraging all employees to accept the importance of achieving the compliance objectives for which they are responsible or accountable;

d) creating an environment where the reporting of noncompliance is encouraged and the reporting employee will be safe from retaliation;

e) encouraging employees to make suggestions that facilitate continual improvement in compliance performance;

f) ensuring compliance is incorporated into the broader organization culture and culture change initiatives;

g) identifying and acting promptly to correct or address noncompliance;

h) ensuring that organizational policies, procedures and processes support and encourage compliance;

i) ensuring that operational objectives and targets do not compromise compliant behaviour.

7.3.2.3 Compliance culture

The development of a compliance culture requires the active, visible, consistent and sustained commitment of the governing body, top management and management towards a common, published standard of behaviour that is required throughout every area of the organization.

EXAMPLE Examples of factors that will support the development of a compliance culture include:

— a clear set of published values;

— management actively seen to be implementing and abiding by the values;

— consistency in the treatment of similar actions, regardless of position;

— mentoring, coaching and leading by example;

— appropriate pre-employment assessment of potential employees;

— an induction or orientation program that emphasizes compliance and the organization's values;

— on-going compliance training, including updates to the training;

— on-going communication on compliance issues;

— performance appraisal systems that consider assessment of compliance behaviour and take into account performance pay to achieve compliance key performance measures and outcomes;

— visible recognition of achievements in compliance management and outcomes;

— prompt and proportionate disciplining in the case of wilful or negligent breaches of compliance obligations;

— a clear link between the organization's strategy and individual roles, reflecting compliance as essential to achieving organizational outcomes;

— open and appropriate communication about compliance.

Evidence of a compliance culture is indicated by the degree to which:

— the items above are implemented;

— stakeholders (particularly employees) believe that the items above have been implemented;

— employees understand the relevance of the compliance obligations related to their own activities and to those of their business unit;

— remediation of noncompliance is 'owned' and actioned at all appropriate levels of the organization as required;

— the role of the compliance function and its objectives are valued;

— employees are enabled and encouraged to raise compliance concerns to the appropriate level of management.

7.4 Communication

7.4.1 General

The organization should determine the need for internal and external communications relevant to the compliance management system, including:

a) on what it will communicate;

b) when to communicate;

c) with whom to communicate;

d) how it will communicate.

NOTE Guidance on internal and external compliance reporting is given in 9.1.7 and 9.1.8.

7.4.2 Internal communication

The organization should adopt appropriate methods of communication to ensure that the compliance message is heard and understood by all employees on an on-going basis. The communication should clearly set out the organization's expectation of employees and those noncompliances that are expected to be escalated and under what circumstances and to whom.

7.4.3 External communication

A practical approach to external communication, targeting all interested parties, should be adopted in accordance with organization policy.

Interested parties can include, but are not limited to, regulatory bodies, customers, contractors, suppliers, investors, emergency services, non-governmental organizations and neighbours.

Methods of communication may include websites and e-mail, press releases, advertisements and periodic newsletters, annual (or other periodic) reports, informal discussions, open days, focus groups, community dialogue, involvement in community events and telephone hotlines. These approaches can encourage understanding and acceptance of an organization's commitment to compliance.

7.5 Documented information

7.5.1 General

The organization's compliance management system should include:

a) documented information recommended by this International Standard;

b) documented information determined by the organization as being necessary for the effectiveness of the compliance management system.

EXAMPLE Examples of documented information include:

— the organization's compliance policy;

— the objectives, targets, structure and content of the compliance management system;

— allocation of roles and responsibilities for compliance;

— register of relevant compliance obligations;

— compliance risk registers and prioritization of the treatment based on the compliance risk assessment process;

— register of noncompliances and near misses;

— annual compliance plans;

— personnel records, including, but not limited to, training records.

NOTE 1 Documented information can include matters relating to regulatory reporting requirements.

NOTE 2 The extent of documented information for a compliance management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of employees;

— the maturity of the compliance management system.

7.5.2 Creating and updating

When creating and updating documented information the organization should ensure appropriate:

— identification and description (e.g. a title, date, author, or reference or version number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

— review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information recommended by the compliance management system and by this International Standard should be controlled to ensure:

a) it is available, accessible and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization should address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention, disposition and disposal;

— the role of third parties in documented information creation and control.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the compliance management system should be identified, as appropriate, and controlled.

Documented information may be prepared for the purpose of obtaining legal advice and therefore may be the subject of legal privilege.

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization should plan, implement and control the processes needed to meet compliance obligations, and to implement the actions determined in 6.1, by:

— defining the objectives of the processes;

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria;

— keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization should control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

8.2 Establishing controls and procedures

Controls should be put in place to manage the identified compliance obligations and associated compliance risk and to achieve desired behaviour.

Effective controls are needed to ensure that the organization's compliance obligations are met and that noncompliances are prevented or detected and corrected. The types and levels of controls should be designed with sufficient rigour to facilitate achieving the compliance obligations that are particular to the organization's activities and operating environment. Such controls should, where possible, be embedded into normal organizational processes.

EXAMPLE Examples of controls include:

— clear, practical and easy to follow documented operating policies, procedures, processes and work instructions;

— systems and exception reports;

— approvals;

— segregation of incompatible roles and responsibilities;

— automated processes;

— annual compliance plans;

— employee performance plans;

— compliance assessments and audits;

— demonstrated management commitment and exemplary behaviour and other measures to promote compliant behaviour;

— active, open and frequent communication on expected behaviour of employees (standards and value, codes of conduct).

These controls should be maintained, periodically evaluated and tested to ensure their continuing effectiveness.

Procedures should be established, documented, implemented and maintained to support the compliance policy and translate the compliance obligations into practice.

In developing these procedures consideration should be given to:

a) integrating the compliance obligations into procedures, including computer systems, forms, reporting systems, contracts and other legal documentation;

b) consistency with other review and control functions in the organization;

c) on-going monitoring and measurement;

d) assessment and reporting (including management supervision) to ensure that employees comply with procedures;

e) specific arrangements for identifying, reporting and escalating instances of noncompliance and risks of noncompliance.

8.3 Outsourced processes

The organization should ensure that outsourced processes are controlled and monitored.

Outsourcing of an organization's operations usually does not relieve the organization of its legal responsibilities or compliance obligations. If there is any outsourcing of the organization's activities, the organization needs to undertake effective due diligence to ensure that its standards and commitment to compliance will not be lowered. Controls over contractors should also be in place to ensure that the contract is complied with effectively (e.g. third-party performance appraisals).

The organization should consider compliance risks related to other third-party-related processes, such as supply of goods and services and distribution of products, and put controls in place, as necessary (e.g. compliance obligations in contractual clauses).

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization should determine:

a) what needs to be monitored and measured and why;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when the monitoring and measuring should be performed;

d) when the results from monitoring and measurement should be analysed, evaluated and reported.

The organization should retain appropriate documented information as evidence of the results.

The organization should evaluate the compliance management system performance and the effectiveness of the compliance management system.

9.1.2 Monitoring

The compliance management system should be monitored to ensure compliance performance is achieved. A plan for continual monitoring should be established, setting out monitoring processes, schedules, resources and the information to be collected.

Compliance monitoring is the process of gathering information for the purpose of assessing the effectiveness of the compliance management system and of the organization's compliance performance.

Monitoring of the compliance management system typically includes:

— effectiveness of training;

— effectiveness of controls, e.g. by sample testing outputs;

— effective allocation of responsibilities for meeting compliance obligations;

— currency of compliance obligations;

— effectiveness in addressing compliance failures previously identified;

— instances where internal compliance inspections are not performed as scheduled.

Monitoring of compliance performance typically includes:

— noncompliance and "near misses" (i.e. incidents without adverse effect);

— instances where compliance obligations are not met;

— instances where objectives are not achieved;

— status of compliance culture;

— leading and lagging indicators established under 9.1.6.

9.1.3 Sources of feedback on compliance performance

The organization should establish, implement, evaluate and maintain procedures for seeking and receiving feedback on its compliance performance from a range of sources, including:

— employees, e.g. through whistle blowing facilities, helplines, feedback, suggestion boxes;

— customers, e.g. through a complaints handling system;

— suppliers;

— regulators;

— process control logs and activity records (including both computer and paper based).

EXAMPLE Examples of feedback on compliance performance include:

— compliance issues,

— noncompliances and compliance concerns,

— emerging compliance issues,

— on-going regulatory and organizational changes and

— comments on compliance effectiveness and performance.

Feedback should serve as a key source of continuous improvement of the compliance management system.

9.1.4 Methods of information collection

There are many methods for collecting information. Each method listed below is relevant in different circumstances and care should be taken to select the variety of tools appropriate to the size, scale, nature and complexity of the organization.

EXAMPLE Examples of information collection include:

— ad hoc reports of noncompliance as they emerge or are identified;

— information gained through hot lines, complaints and other feedback, including whistle blowing;

— informal discussions, workshops and focus groups;

— sampling and integrity testing, such as mystery shopping;

— results of perception surveys;

— direct observations, formal interviews, facility tours and inspections;

— audits and reviews;

— stakeholder queries, training requests and feedback provided during training (particularly those of employees).

9.1.5 Information analysis and classification

Effective classification and management of the information is critical.

A system should be developed for classifying, storing and retrieving the information.

EXAMPLE Examples of information classification criteria include:

— source;

— department;

— noncompliance description;

— obligation references;

— indicators;

— severity;

— actual or potential impact.

The information management systems should capture both issues and complaints and allow classification and analysis of those that relate to compliance.

Once the information has been collected, it needs to be analysed and critically assessed to identify root causes and appropriate actions to be taken. The analysis should consider systemic and recurring problems for rectification or improvement as these are likely to carry significant compliance risks for the organization and can be more difficult to identify.

9.1.6 Development of indicators

It is important that organizations develop a set of measurable indicators that will assist the organization in measuring achievement of its objectives (see 6.2) and quantifying its compliance performance. This process should take into account the results of the assessment of compliance risks (see 4.6) to ensure that indicators relate to the relevant characteristics of the compliance risks of the organization. The issue of what and how to measure compliance performance can be challenging in some aspects, but is nevertheless a vital part of demonstrating the effectiveness of the compliance management system. Furthermore, the indicators needed will vary with the organization's maturity and the timing and extent of new and revised programs being implemented.

EXAMPLE 1 Examples of activity indicators include:

— percentage of employees trained effectively;

— frequency of contacts by regulators;

— usage of feedback mechanisms (including comments on the value of those mechanisms by users);

— what type of corrective action was undertaken for each noncompliance.

EXAMPLE 2 Examples of reactive indicators include:

— issues and noncompliance identified, reported by type, area and frequency;

— consequence of noncompliance, which can include valuation of impact resulting from monetary compensation, fines and other penalties, cost of remediation, reputation or cost of employees' time;

— the amount of time taken to report and take corrective action;

EXAMPLE 3 Examples of predictive indicators include:

— risks of non-compliances (measured as potential loss/gain of objectives (revenue, health and safety, reputation etc.) over time

— non-compliance trends (expected compliance rate based on past trends)

9.1.7 Compliance reporting

The governing body, management and the compliance function should ensure that they are effectively informed on the performance of the organization's compliance management system and of its continuing adequacy, including all relevant noncompliances, in a timely manner and actively promote the principle that the organization encourages and supports a culture of full and frank reporting. Internal reporting arrangements should ensure that:

a) appropriate criteria and obligations for reporting are set out;

b) timelines for regular reporting are established;

c) an exception reporting system is in place which facilitates ad hoc reporting of emerging noncompliance;

d) systems and processes are in place to ensure the accuracy and completeness of information;

e) accurate and complete information is provided to the correct functions or areas of the organization to enable preventative, corrective and remedial action to be taken;

f) there is sign-off on the accuracy of reports to the governing body, including by the compliance function.

An organization should choose a format, content and timing of its internal compliance reporting that is appropriate to its circumstances, unless otherwise specified by law.

Reporting on compliance should be incorporated in standard organizational reports.

Separate reports should only be prepared for major noncompliance and for emerging issues.

All noncompliance need to be appropriately reported. While the reporting of systemic and recurring problems is particularly important, a one-off noncompliance can be of equal concern if it is major or deliberate. Even a small failure may indicate serious weakness in the current process and the compliance management system. If not reported in a timely manner, it can lead to the view that the failure does not matter and can result in such failure becoming a systemic problem.

Employees should be encouraged to respond and report noncompliance with the law and other incidents of noncompliance, and to see reporting as a positive and non-threatening action without fear of retaliation.

Reporting obligations should be set out clearly in the organization's compliance policy and procedures and reinforced by other methods, such as informal reinforcement by managers during their day-to-day work with employees.

9.1.8 Content of compliance reports

Compliance reports can include:

a) any matters which the organization is required to notify to any regulatory authority;

b) changes in compliance obligations, their impact on the organization and the proposed course of action to meet the new obligations;

c) measurement of compliance performance, including noncompliance and continual improvement;

d) number and details of possible noncompliance(s) and a subsequent analysis of them;

e) corrective actions undertaken;

f) information on the compliance management system's effectiveness, achievements and trends;

g) contacts, and developments in relationships, with regulators;

h) results from audits, as well as monitoring activities.

The compliance policy should promote the immediate reporting of materially significant matters which arise outside the timelines for regular reporting.

9.1.9 Record-keeping

Accurate, up-to-date records of the organization's compliance activities should be maintained to assist in the monitoring and review process and demonstrate conformity with the compliance management system.

Record-keeping should include recording and classifying complaints, disputes and alleged noncompliance and the steps taken to resolve them.

Records should be stored in a manner that ensures they remain legible, readily identifiable and retrievable.

These records should be protected against any addition, deletion, modification, unauthorized use or concealment.

The organization's compliance management system records can include:

a) information on compliance performance, including compliance reports;

b) complaints, their resolution and communications from interested parties;

c) details of noncompliance and corrective and preventive actions;

d) results of reviews and audits of the compliance management system and actions taken.

9.2 Audit

The organization should conduct audits at least at planned intervals to provide information on whether the compliance management system:

a) conforms to:

   1) the organization's own criteria for its compliance management system;

   2) the recommendations of this International Standard;

b) is effectively implemented and maintained.

Additional audits can also be conducted as required.

The organization should:

— plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) should take into consideration the importance of the processes concerned and the results of previous audits;

— define the audit criteria and scope for each audit;

— select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

— ensure that the results of the audits are reported to relevant management;

— retain documented information as evidence of the implementation of the audit programme and the audit results.

9.3 Management review

Top management should review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The actual depth and frequency of such reviews will vary with the nature of the organization and its policies.

The management review should include consideration of:

a) the status of actions from previous management reviews;

b) the adequacy of the compliance policy;

c) the extent to which the compliance objectives have been met;

d) adequacy of resources;

e) changes in external and internal issues that are relevant to the compliance management system;

f) information on the compliance performance, including trends in:

- nonconformities, corrective actions and timelines for resolution;
- monitoring and measurement results,
- communication from interested parties, including complaints;
- audit results;

g) opportunities for continual improvement.

The outputs of the management review should include decisions related to continual improvement opportunities and any need for changes to the compliance management system.

It should include also recommendations on:

a) the need for changes to the compliance policy, its associated objectives, systems, structure and personnel;

b) changes to compliance processes to ensure effective integration with operational practices and systems;

c) areas to be monitored for potential future noncompliance;

d) corrective actions with respect to noncompliance;

e) gaps or lack in current compliance systems and longer term continual improvement initiatives;

f) recognition of exemplary compliance behaviour within the organization.

The organization should retain documented information as evidence of the results of management reviews and a copy should be provided to the governing body.

10 Improvement

10.1 Nonconformity, noncompliance and corrective action

10.1.1 General

When a nonconformity and/or noncompliance occurs, the organization should:

a) react to the nonconformity and/or noncompliance and, as applicable:

- take action to control and correct it; and/or
- manage the consequences;

b) evaluate the need for action to eliminate the root causes of the nonconformity and/or noncompliance, in order that it does not recur or occur elsewhere, by:

- reviewing the nonconformity and/or noncompliance;
- determining the causes of the nonconformity and/or noncompliance;
- determining if similar nonconformities and/or noncompliances exist; or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the compliance management system, if necessary.

The failure to prevent or detect a one-off noncompliance does not necessarily mean that the compliance management system is not generally effective in preventing and detecting noncompliance.

Corrective actions should be appropriate to the effects of the nonconformities and/or noncompliances encountered. The organization should retain documented information as evidence of:

— the nature of the nonconformities and/or noncompliances and any subsequent actions taken;

— the results of any corrective action.

Information from analysing nonconformity and/or noncompliance can be used to consider:

— assessing product and service performance;

— improving and/or redesigning products and services;

— changing organizational practices and procedures;

— retraining employees;

— re-assessing the need to inform interested parties;

— providing early warning of potential noncompliance;

— redesigning or reviewing controls;

— enhancing notification and escalation steps (internal and external).

10.1.2 Escalation

A clear and timely escalation process should be adopted and communicated to ensure that all noncompliances are raised, reported and eventually escalated to relevant management, and that the compliance function is informed and able to support the escalation. Where appropriate, escalation should be to top management and the governing body, including relevant committees. The process should specify to whom, how and when issues are to be reported and the timelines for internal and external reporting.

When organizations are required by law to report noncompliance, regulatory authorities need to be informed in accordance with the applicable regulations or as otherwise agreed.

Even if organizations are not required by law to report noncompliance, they may consider voluntary self-disclosure of noncompliance to regulatory authorities to mitigate the consequences of noncompliance.

An effective compliance management system should include a mechanism for an organization's employees and/or others to report suspected or actual misconduct or violations of the organization's compliance obligations on a confidential basis and without fear of retaliation.

10.2 Continual improvement

The organization should seek to continually improve the suitability, adequacy and effectiveness of the compliance management system.

The information collected, analysed and evaluated accordingly, and included in compliance reports, should be used as basis to identify opportunities for improvement of compliance performance of the organization.

Bibliography

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 10002, *Quality management — Customer satisfaction — Guidelines for complaints handling in organizations*

[3] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[4] ISO 19011, *Guidelines for auditing management systems*

[5] ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*

[6] ISO 26000, *Guidance on social responsibility*

[7] ISO 31000, *Risk management — Principles and guidelines*

[8] ISO Guide 73:2009, *Risk management — Vocabulary*

ICS 03.100.01

Price based on 28 pages