Compliance management systems — Requirements with guidance for use

1 Scope

This document specifies requirements and provides guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization.

This document is applicable to all types of organizations regardless of the type, size and nature of the activity, as well as whether the organization is from the public, private or non-profit sector.

All requirements specified in this document that refer to a governing body apply to top management in cases where an organization does not have a governing body as a separate function.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.6)

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.

Note 2 to entry: If the organization is part of a larger entity, the term "organization" refers only to the part of the larger entity that is within the scope of the compliance management system.

3.2
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.1) that can affect, be affected by, or perceive itself 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* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: For the purposes of this document, the term "top management" refers to the highest level of executive management.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.5) and *objectives* (3.6) as well as *processes* (3.8) to achieve those objectives

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

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

3.5
policy
intentions and direction of an *organization* (3.1), as formally expressed by its *top management* (3.3)

Note 1 to entry: A policy can also be formally expressed by an organization's *governing body* (3.2).

3.6
objective
result to be achieved

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

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide, or specific to a project, product, service or *process* (3.8)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, a purpose, an operational criterion, as a *compliance* (3.7) 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* (3.4), compliance objectives are set by the *organization* (3.1), consistent with the compliance *policy* (3.5), to achieve specific results.

3.7
risk
effect of uncertainty on objectives

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) and "consequences" (as defined in ISO Guide 73), 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) of occurrence.

3.8
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called output, product or service depends on the context of the reference.

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
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* (3.4), including related *processes* (3.8);

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

— evidence of results achieved (records).

3.11
performance
measurable result

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

Note 2 to entry: Performance can relate to managing activities, *processes* (3.8), products, services, systems or *organizations* (3.1).

3.12
continual improvement
recurring activity to enhance *performance* (3.11)

3.13
effectiveness
extent to which planned activities are realized and planned results are achieved

3.14
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* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.10).

3.15
conformity
fulfilment of a *requirement* (3.14)

3.16
nonconformity
non-fulfilment of a *requirement* (3.14)

Note 1 to entry: A nonconformity is not necessarily a *noncompliance* (3.27).

3.17
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.16) and to prevent recurrence

3.18
audit
systematic and independent *process* (3.8) for obtaining 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* (3.30)), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

Note 4 to entry: Independence can be demonstrated by the freedom from responsibility for the activity being audited or freedom from bias and conflict of interest.

3.19
measurement
process (3.8) to determine a value

3.20
monitoring
determining the status of a system, a *process* (3.8) or an activity

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

3.21
governing body
person or group of persons that has the ultimate responsibility and authority for an *organization's* (3.1) activities, governance and *policies* (3.5) and to which *top management* (3.3) reports and by which top management is held accountable

Note 1 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management.

Note 2 to entry: A governing body can include, but is not limited to, a board of directors, committees of the board, a supervisory board or trustees.

3.22
personnel
individuals in a relationship recognized as a work relationship in national law or practice, or in any contractual relationship that depends on its activity from the *organization* (3.1)

3.23
compliance function
person or group of persons with responsibility and authority for the operation of the *compliance* (3.26) *management system* (3.4)

Note 1 to entry: Preferably one individual will be assigned to the oversight of compliance management system.

3.24
compliance risk
likelihood of occurrence and the consequences of *noncompliance* (3.27) with the *organization's* (3.1) *compliance obligations* (3.25)

3.25
compliance obligations
requirements (3.14) that an *organization* (3.1) mandatorily has to comply with as well as those that an organization voluntarily chooses to comply with

3.26
compliance
meeting all the *organization's* (3.1) *compliance obligations* (3.25)

3.27
noncompliance
non-fulfilment of *compliance obligations* (3.25)

3.28
compliance culture
values, ethics, beliefs and *conduct* (3.29) 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* (3.26)

3.29
conduct
behaviours and practices that impact outcomes for customers, employees, suppliers, markets and communities

3.30
third party
person or body that is independent of the *organization* (3.1)

Note 1 to entry: All business associates are third parties, but not all third parties are business associates.

3.31
procedure
specified way to carry out an activity or a *process* (3.8)

[SOURCE: ISO 9000:2015, 3.4.5]

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its compliance management system.

For this purpose, the organization shall consider a broad range of issues, not limited to:

— the business model, including strategy, nature, size and scale complexity and sustainability of the organization's activities and operations;

— the nature and scope of business relations with third parties;

— the legal and regulatory context;

— the economic situation;

— social, cultural and environmental contexts;

— internal structures, policies, processes, procedures and resources, including technology;

— its compliance culture.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

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

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the compliance management system.

4.3 Determining the scope of the compliance management system

The organization shall 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 main compliance risks the organization is facing and the geographical or organizational boundaries, or both, to which the compliance management system will apply, especially if the organization is a part of a larger entity.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2, 4.4 and 4.5.

The scope shall be available as documented information.

4.4 Compliance management system

The organization shall establish, implement, maintain and continually improve a compliance management system, including the processes needed and their interactions, in accordance with the requirements of this document.

The compliance management system shall reflect the organization's values, objectives, strategy and compliance risks, taking into account the context of the organization (see 4.1).

4.5 Compliance obligations

The organization shall systematically identify its compliance obligations resulting from its activities, products and services, and assess their impact on its operations.

The organization shall have processes in place to:

a) identify new and changed compliance obligations to ensure ongoing compliance;

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

The organization shall maintain documented information of its compliance obligations.

4.6 Compliance risk assessment

The organization shall identify, analyse and evaluate its compliance risks based upon a compliance risk assessment.

The organization shall identify compliance risks by relating its compliance obligations to its activities, products, services and relevant aspects of its operations.

The organization shall assess compliance risks related to outsourced and third-party processes.

The compliance risks shall be assessed periodically and whenever there are material changes in circumstances or organizational context.

The organization shall retain documented information on the compliance risk assessment and on the actions to address its compliance risks.

5 Leadership

5.1 Leadership and commitment

5.1.1 Governing body and top management

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

— ensuring that the compliance policy and compliance objectives are established and are compatible with the strategic direction of the organization;

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

— ensuring that the resources needed for the compliance management system are available;

— communicating the importance of effective compliance management and of conforming to the compliance management system requirements;

— ensuring that the compliance management system achieves its intended result(s);

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

— promoting continual improvement;

— supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

The governing body and top management shall:

— establish and uphold the values of the organization;

— ensure that policies, processes and procedures are developed and implemented to achieve compliance objectives;

— ensure that they are informed in a timely manner on compliance matters, including on instances of noncompliance, and ensure that appropriate action is taken;

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

— ensure that compliance responsibilities are included in job descriptions as appropriate;

— appoint or nominate a compliance function (see 5.3.2);

— ensure that a system for raising and addressing concerns in accordance with 8.3 is established.

5.1.2 Compliance culture

The organization shall develop, maintain and promote a compliance culture at all levels within the organization.

The governing body, top management and management shall demonstrate an active, visible, consistent and sustained commitment towards a common standard of behaviour and conduct that is required throughout the organization.

Top management shall encourage behaviour that creates and supports compliance. It shall prevent and not tolerate behaviour that compromises compliance.

5.1.3 Compliance governance

The governing body and top management shall ensure that the following principles are implemented:

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

— independence of the compliance function;

— appropriate authority and competence of the compliance function.

NOTE 1 Direct access can include: direct reporting line to the governing body, submitting periodic reports to the governing body and participation in its meetings.

NOTE 2 Independence means absence from any undue interference or pressure, or both, with the operation of the compliance function.

5.2 Compliance policy

The governing body and top management shall establish a compliance policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting compliance objectives;

c) includes a commitment to meet applicable requirements;

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

The compliance policy shall:

— be aligned with the organization's values, objectives and strategy;

— require compliance with the organization's compliance obligations;

— support the compliance governance principles in accordance with 5.1.3;

— make reference to and describe the compliance function;

— outline the consequences of not complying with the organization's compliance obligations, policies, processes and procedures;

— encourage the raising of concerns and prohibit any form of retaliation;

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

— be appropriately implemented and enforced;

— be available as documented information;

— be communicated within the organization;

— be available to interested parties, as appropriate.

5.3 Roles, responsibilities and authorities

5.3.1 Governing body and top management

The governing body and top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

The governing body and top management shall assign the responsibility and authority for:

a) ensuring that the compliance management system conforms to the requirements of this document;

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

The governing body shall:

— ensure that top management is measured against the achievement of compliance objectives;

— exercise oversight over top management regarding the operation of the compliance management system.

Top management shall:

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

— ensure that effective systems of timely reporting on compliance performance are in place;

— ensure alignment between strategic and operational targets and compliance obligations;

— establish and maintain accountability mechanisms including disciplinary actions and consequences;

— ensure the integration of compliance performance into performance appraisals of personnel.

5.3.2 Compliance function

The compliance function shall be responsible for the operation of the compliance management system including the following:

— facilitating the identification of compliance obligations;

— documenting the compliance risk assessment (see 4.6);

— aligning the compliance management system with the compliance objectives;

— monitoring and measuring compliance performance;

— analysing and evaluating the performance of the compliance management system to identify any need for corrective action;

— establishing a compliance reporting and documenting system;

— ensuring the compliance management system is reviewed at planned intervals (see 9.2 and 9.3);

— establishing a system for raising concerns and ensuring that concerns are addressed.

The compliance function shall exercise oversight that:

— responsibilities to achieve identified compliance obligations are appropriately allocated throughout the organization;

— compliance obligations are integrated into policies, processes and procedures;

— all relevant personnel are trained as required;

— compliance performance indicators are established.

The compliance function shall provide:

— personnel with access to resources on compliance policies, processes and procedures;

— advice to the organization on compliance-related matters.

NOTE The specific duties of the compliance function do not relieve other personnel of their responsibilities for compliance.

The organization shall ensure that the compliance function is given access to:

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

— all levels of the organization;

— all personnel, documented information and data needed;

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

5.3.3 Management

Management shall be responsible for compliance within its area of responsibility by:

— cooperating with and supporting the compliance function and encouraging personnel to do the same;

— ensuring that all personnel within their control are complying with the organization's compliance obligations, policies, processes and procedures;

— identifying and communicating compliance risks in their operations;

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

— attending and supporting compliance training activities;

— developing personnel awareness of compliance obligations and directing them to meet training and competence requirements;

— encouraging their personnel to raise compliance concerns and supporting them and precluding any form of retaliation;

— actively participating in the management and resolution of compliance-related incidents and issues as required;

— ensuring that, once the need for corrective action is identified, appropriate corrective action is recommended and implemented.

5.3.4 Personnel

All personnel shall:

— adhere to the organization's compliance obligations, policies, processes and procedures;

— report compliance concerns, issues and failures;

— participate in training as required.

6 Planning

6.1 Actions to address risks and opportunities

When planning for the compliance management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

— give assurance that the compliance management system can achieve its intended result(s);

— prevent, or reduce, undesired effects;

— achieve continual improvement.

When planning for the compliance management system, the organization shall consider:

— its compliance objectives (see 6.2);

— the compliance obligations identified (see 4.4);

— the results of the compliance risk assessment (see 4.5).

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

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

   2) evaluate the effectiveness of these actions.

6.2 Compliance objectives and planning to achieve them

The organization shall establish compliance objectives at relevant functions and levels.

The compliance objectives shall:

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 as appropriate;

g) be available as documented information.

When planning how to achieve its compliance objectives, the organization shall 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.

6.3 Planning of changes

When the organization determines the need for changes to the compliance management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the compliance management system.

7.2 Competence

7.2.1 General

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its compliance performance;

— ensure that these persons are competent on the basis of appropriate education, training, or experience;

— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.2.2 Employment process

In relation to all its personnel, the organization shall develop, establish, implement and maintain processes such that:

a) conditions of employment require personnel to comply with the organization's compliance obligations, policies, processes and procedures;

b) within a reasonable period of their employment commencing, personnel receive a copy of, or are provided with access to, the compliance policy and training in relation to that policy;

c) appropriate disciplinary action shall be taken against personnel who violate the organization's compliance obligations, policies, processes and procedures.

As part of the employment process, the organization shall consider the compliance risks posed by roles and by personnel and apply due diligence procedures as required prior to any hiring, transfer and promotion.

The organization shall implement a process that provides for a periodic review of performance targets, performance bonuses and other incentives, to verify that there are appropriate measures in place to prevent encouraging noncompliance.

7.2.3 Training

The organization shall provide relevant personnel with training on a regular basis, from the time of commencement of employment and at planned intervals determined by the organization.

Training shall be:

a) appropriate to the roles of personnel and the compliance risks to which personnel are exposed;

b) assessed for effectiveness;

c) reviewed regularly.

Taking into account the compliance risks identified, the organization shall ensure procedures are implemented to address compliance awareness and training for third parties acting on its behalf and which can pose a compliance risk to the organization.

Training records shall be retained as documented information.

7.3 Awareness

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

— the compliance policy;

— their contribution to the effectiveness of the compliance management system, including the benefits of improved compliance performance;

— the implications of not conforming with the compliance management system requirements.

— the means of and procedures for raising compliance concerns (see 8.3);

— the relation of the compliance policy and the compliance obligations relevant to their role;

— the importance of supporting compliance culture.

7.4 Communication

The organization shall determine the 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 to communicate.

The organization shall:

— consider aspects of diversity and potential barriers when considering its communication needs;

— ensure that the views of interested parties are considered in establishing its communication process(es);

— when establishing its communication process(es):

  — include communication on its compliance culture, compliance objectives and obligations;

  — ensure that compliance information to be communicated is consistent with information generated within the compliance management system and is reliable;

— respond to relevant communications on its compliance management system;

— retain documented information as evidence of its communications, as appropriate;

— internally communicate information relevant to the compliance management system among the various levels and functions of the organization, including changes to the compliance management system, as appropriate;

— ensure its communication process(es) enables personnel to contribute to continual improvement of the compliance management system;

— ensure its communication process(es) enables personnel to raise concerns (see 8.3);

— externally communicate information relevant to the compliance management system, as established by the organization's communication process(es), and include communication on its compliance culture, compliance objectives and obligations.

7.5 Documented information

7.5.1 General

The organization's compliance management system shall include:

a) documented information required by this document;

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

NOTE 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 persons.

7.5.2 Creating and updating documented information

When creating and updating documented information, the organization shall ensure appropriate:

— identification and description (e.g. a title, date, author, or reference 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 required by the compliance management system and by this document shall be controlled to ensure:

a) it is available, 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 shall 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 and disposition.

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

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

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

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

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

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

The organization shall ensure that externally provided processes, products or services, that are relevant to the compliance management system, are controlled.

NOTE Outsourcing of an organization's operations does not relieve the organization of its legal responsibilities or compliance obligations.

The organization shall ensure that third-party processes are controlled and monitored.

8.2 Establishing controls and procedures

The organization shall implement controls to manage its compliance obligations and associated compliance risks. These controls shall be maintained, periodically reviewed and tested to ensure their continuing effectiveness.

NOTE Testing controls means conducting a designed exercise to see whether the control does what was intended or cannot be bypassed or is actually effective in reducing the impact or likelihood of the risk.

8.3 Raising concerns

The organization shall establish, implement and maintain a process to encourage and enable the reporting of (in cases of reasonable grounds to believe that the information is true) attempted, suspected or actual violations of the compliance policy or compliance obligations.

This process shall:

— be visible and accessible throughout the organization;

— treat reports confidentially;

— accept anonymous reports;

— protect those making reports from retaliation;

— enable personnel to receive advice.

The organization shall ensure that all personnel are aware of the reporting procedures, their rights and protections and are able to use them.

8.4 Investigation processes

The organization shall develop, establish, implement and maintain processes to assess, evaluate, investigate and close reports on suspected or actual instances of noncompliance. These processes shall ensure fair and impartial decision-making.

The investigation processes shall be carried out independently and without conflict of interests by competent personnel.

The organization shall use the outcome of investigations for the improvement of the compliance management system as appropriate (see Clause 10).

The organization shall regularly report on the numbers and outcomes of investigations to the governing body or top management.

The organization shall retain documented information on the investigation.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization shall monitor the compliance management system to ensure compliance objectives are achieved.

The organization shall determine:

— what needs to be monitored and measured;

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

— when the monitoring and measuring shall be performed;

— when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

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

9.1.2 Sources of feedback on compliance performance

The organization shall establish, implement, evaluate and maintain processes for seeking and receiving feedback on its compliance performance from a range of sources. The information shall be analysed and critically assessed to identify root causes for noncompliance, ensure appropriate actions are taken, and reflect this information in the periodic risk assessment required in 4.5.

9.1.3 Development of indicators

The organization shall develop,implement and maintain a set of appropriate indicators that will assist the organization in evaluating the achievement of its compliance objectives and assessing its compliance performance.

9.1.4 Compliance reporting

The organization shall establish, implement and maintain processes for compliance reporting to ensure that:

a) appropriate criteria for reporting are defined;

b) timelines for regular reporting are established;

c) an exception reporting system is implemented that facilitates ad hoc reporting;

d) systems and processes are implemented 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 preventive, corrective and remedial action to be taken in a timely manner.

Any reports issued by the compliance function to the governing body or top management shall be adequately protected from alteration.

9.1.5 Record-keeping

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

9.2 Internal audit

9.2.1 General

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

a) conforms to:

   — the organization's own requirements for its compliance management system;

   — the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s) including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit objectives, criteria and scope for each audit;

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

c) ensure that the results of the audits are reported to relevant managers and to management.

NOTE 1 Relevant management can include the compliance function, top management and the governing body.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

NOTE 2 Guidance on auditing management systems is given in ISO 19011.

9.3 Management review

9.3.1 General

Governing body and top management shall review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include:

a) the status of actions from previous management reviews;

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

c) changes in needs and expectations of interested parties that are relevant to the compliance management system;

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

   — nonconformities, noncompliances and corrective actions;

   — monitoring and measurement results;

   — audit results;

e) opportunities for continual improvement.

The management review shall take into account:

— the adequacy of the compliance policy;

— the independence of the compliance function;

— the extent to which the compliance objectives have been met;

— the adequacy of resources;

— adequacy of the compliance risks assessment;

— the effectiveness of existing controls and performance indicators;

— communication from persons raising concerns, interested parties, including feedback (see 9.1.2) and complaints;

— investigations (see 8.4);

— the effectiveness of the reporting system.

9.3.3 Management review results

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

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the compliance management system.

When the organization determines the need for changes to the compliance management system, the changes shall be carried out in a planned manner.

The organization shall consider:

— the purpose of the changes and their potential consequences;

— the design and operational effectiveness of the compliance management system;

— the availability of adequate resources;

— the allocation or reallocation of responsibilities and authorities.

10.2 Nonconformity and corrective action

When a nonconformity or noncompliance occurs, the organization shall:

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

   1) take action to control and correct it;

   2) deal with the consequences;

b) evaluate the need for action to eliminate the cause(s) of the nonconformity or noncompliance, or both, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity and or noncompliance, or both;

   2) determining the causes of the nonconformity or noncompliance, or both;

   3) determining if similar nonconformities or noncompliances, or both, exist, or can 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.

Corrective actions shall be appropriate to the effects of the nonconformities or noncompliance, or both, encountered.

Documented information shall be available as evidence of:

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

— the results of any corrective action.

Annex A
(informative)

Guidance for the use of this document

A.1 Background and Scope

A.1.1 General

The purpose of the guidance in this annex is to indicate approaches and types of actions that an organization can take when implementing its compliance management system. It is not intended to be comprehensive or prescriptive, nor is an organization obliged to implement all the suggestions in this guidance in order to have a compliance management system that meets the requirements of this document. The steps taken by the organization should be reasonable with regard to the nature and extent of compliance risks it faces to meet its compliance obligations.

An organization can choose to implement this compliance management system as a separate system, however, ideally it would be implemented in conjunction with its other management systems, such as risk, anti-bribery, quality, environmental, information security and social responsibility, just to give a few examples. In which case the organization can refer to ISO 31000, ISO 37001, ISO 9001, ISO 14001 and ISO/IEC 27001, as well as ISO 26000.

A.1.2 Scope

Organizations of any size, complexity or industry can apply this document to create a compliance management system by following its requirements. This will give them an understanding of their context, business operations, resulting obligations and compliance risks and assist them in implementing reasonable steps to meet their obligations. Each of the requirements in the document shall be followed. However, the guidance in this annex is simply recommended.

In practice, it is often easier to implement a compliance management system in line with this document in small organizations, because they are less complex. Small and medium-sized organizations will enhance their organizational practices by using the principles of the requirements of this document.

This document refers to governing body and top management and defines what these terms mean in a variety of contexts and locations. This document can be used by all organizations so if a particular organization does not use these terms, look to the intent of their use: the requirements or instructions will apply to the person or group of persons who have the authority and responsibility at the pinnacle of the organization.

A.2 Normative references

This document has no normative references. Users can refer to the bibliography for other information and International Standards that are relevant to compliance.

A.3 Terms and definitions

This document has adopted the high level structure (HLS) developed by ISO to improve alignment among its International Standards for management systems. The HLS structure sets out the clause sequence, common terminology and definitions, and identical core text that form the nucleus of ISO management system standards (MSS). This means that some of the definitions can be used in a way that is not familiar. The definitions provided can provide clarification when using this document.

This common approach to MSS increases the value of such standards to users. It is particularly useful for those organizations that choose to operate a single (sometimes called "integrated") management system that can meet the requirements of two or more MSS simultaneously. Organizations that have not adopted MSS or a compliance management framework can easily adopt this document as stand-alone guidance within their organization.

Further information on MSS and the HLS structure can be found at: https://www.iso.org/management-system-standards.html.

A.4 Context of the organization

A.4.1 Understanding the organization and its context

The intent of the clause is that organizations establish a high-level (e.g. strategic) understanding of the important issues that can affect their compliance management system. The knowledge gained is then used to guide the approach to planning, implementing, operating and improving the compliance management system.

This is the process of reviewing all information available about the organization: what it does, where, how and why. External and key factors are assessed for their impact on the organization in terms of its compliance obligations.

The most obvious of these compliance obligations arise from the legal and regulatory contexts an organization operates in, but obligations or risks can also arise from other factors as suggested in this document. An organization should also consider relevant future trends that can have an impact.

Internal factors should be taken into consideration. Some examples are included in the document. This list is not exhaustive, and there can be others that will be relevant to an organization.

A.4.2 Understanding the needs and expectations of interested parties

Organizations should establish an understanding of the needs and expectations of the people or organizations that can affect, be affected by or perceive themselves to be affected by the compliance management system.

Some are mandatory because they have been incorporated into formal requirements, such as laws, regulations, permits and licenses, and governmental or court action. There can be other formal requirements not included here that apply.

Other needs and expectations of an interested party become obligations when they are specified, and the organization decides that it will adopt them voluntarily by entering into an agreement or contract. Once the organization has decided on them, they become compliance obligations.

Examples of external interested parties include:

— governments and government agencies;

— regulatory bodies;

— customers;

— contractors;

— suppliers;

— third-party intermediaries;

— owners, shareholders and investors;

— non-governmental organizations;

— society and community groups

— business associates.

Examples of internal interested parties include:

— the governing body;

— management;

— employees;

— internal functions such as risk management, internal control, internal audit, human resources.

A.4.3 Determining the scope of the compliance management system

Determining the scope of a compliance management system is the process whereby organizations establish the physical and organizational boundaries to which the compliance management system will apply. In doing so, the organization has the freedom and flexibility to choose to implement the compliance management system within the entire organization, a specific unit or specific function(s) within an organization.

Typically, a compliance management system will be implemented in the entire organization and, in cases of groups of organizations, in the entire group of organizations to avoid double standards of ethical conduct and compliance.

The scope should be reasonable and proportionate, taking into account the nature and extent of compliance risks faced by the organization.

An understanding of the context and the requirements of relevant interested parties is a consideration when establishing the scope of the compliance management system and when determining which requirements the organization will adopt.

A.4.4 Compliance management system

A compliance management system is a framework that integrates essential structures, policies, processes and procedures to achieve the desired compliance outcomes, and act to prevent, detect and respond to noncompliance.

Typically, a compliance management system framework is a structural matter: the necessary infrastructure on which to build this system. It then needs to be made operational through the implementation of policies, processes and procedures. Then it needs to be maintained and continually improved.

There are many elements to a compliance management system. Some elements of the management system will be designed to support desired behaviours, while others will be designed to prevent undesirable behaviours. Some elements are solely to monitor the compliance performance of the organization or provide alerts if noncompliance take place.

The compliance management system will recognize that mistakes do happen and will have processes to ensure there is appropriate reaction. An appropriate reaction will include remediation of processes, systems and impacted parties.

The compliance management system should be based on the principles of good governance, proportionality, integrity, transparency, accountability and sustainability.

The compliance management system should be available as documented information.

A.4.5 Compliance obligations

The organization should take compliance obligations as a basis for establishing, developing, implementing, evaluating, maintaining and improving its compliance management system.

Requirements that an organization mandatorily must comply with can 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.

Requirements that an organization voluntarily chooses to comply with can 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.

The organization should identify compliance obligations by departments, functions and different types of organizational activities in order to determine who is affected by these compliance obligations.

Processes to obtain information on changes to laws and other compliance obligations can 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, court decisions).

A risk-based approach should be taken, i.e. organizations should start with the identification of the most important compliance obligation that is relevant to the business and then focus on all the other compliance obligations (pareto principle).

Where appropriate, the organization should establish and maintain a single document (such as a register or log) setting out all of its compliance obligations and have a process for updating the document on a regular basis.

In addition to setting out the compliance obligations, the document should include, but not be limited to:

— the impact of the compliance obligations;

— the management of the compliance obligations;

— controls linked to the compliance obligations;

— risk assessment.

A.4.6 Compliance risk assessment

The compliance risk assessment constitutes the basis for the implementation of the compliance management system and the allocation of appropriate and adequate resources and processes to manage identified compliance risks.

Compliance risks can be characterized by the likelihood of occurrence and the consequences of noncompliance with the organization's compliance policy and obligations.

Compliance risks include inherent compliance risks and residual compliance risks. The inherent compliance risks refer to all compliance risks faced by an organization in an uncontrolled state without any corresponding compliance risk treatment measures. The residual compliance risks are the compliance risks not effectively controlled by the existing compliance risk treatment measures of an organization.

The organization should analyse compliance risks by considering the root causes and sources of noncompliance and the consequence of these, while including the likelihood that these ramifications can occur. Consequences can include, for example, personal and environmental harm, economic loss, reputational harm, administrative changes, and civil and criminal liabilities.

The identification of compliance risks includes the identification of compliance risk sources and the definition of compliance risk situations. Organizations should identify the compliance risk sources within various departments, functions and different types of organizational activities in accordance with the department responsibilities, job responsibilities and different types of organizational activities. The organization should regularly identify compliance risk sources and define the compliance risk situations corresponding to each compliance risk source to develop a list of compliance risk sources and a list of compliance risk situations.

Risk assessment involves comparing the level of compliance risk that is acceptable to the organization with the level of compliance risk set out in the compliance policy.

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;

— mergers and acquisitions;

— noncompliance(s) (even a single incident of noncompliance can constitute a material change in circumstances and near-misses).

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).

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 focusing 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 and treatment.

When conducting a risk assessment (see ISO 31000 for guidance) attention should be paid to appropriate techniques (as detailed in IEC 31010).

A.5 Leadership

A.5.1 Leadership and commitment

A.5.1.1 Governing body and top management

Effective compliance requires an active commitment from the governing body and top management that permeates the whole organization.

It is vital for the compliance management system that the governing body and top management clearly and visibly demonstrate their commitment to achieving the goals of the compliance management system.

Noncompliance can result in a negative impact to the business, such as reputational damage, loss of licence to operate, loss of opportunity, and significant cost. Therefore, the governing body and top management should acknowledge the strategic importance of effective compliance management.

The document lists many ways that leadership can demonstrate their commitment. The most fundamental way is through active and visible support for the establishment and maintenance of the compliance management system.

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 personnel that the organization will meet its compliance obligations;

— the commitment to compliance is communicated widely to all personnel and relevant interested parties in clear and convincing statements supported by action;

— the compliance function has staff with the appropriate competence, status authority and independence that reflects the importance of effective compliance and has direct access to the governing body;

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

— policies, processes and procedures 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;

— a regular review of the compliance management system is undertaken (recommended at least annually);

— the compliance performance of the organization is continually improved;

— corrective action is taken in a timely manner

— the governing body and the top management are following the organization's compliance management system.

A.5.1.2 Compliance culture

Factors that will support the development of a compliance culture can include:

— a clear set of published values;

— management actively and visibly implementing and abiding by the values;

— consistency in the treatment of noncompliances, regardless of position;

— mentoring, coaching and leading by example;

— an appropriate pre-employment assessment of potential personnel for critical functions including due diligence;

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

— ongoing compliance training, including updates to the training to all personnel and relevant interested parties;

— ongoing communication on compliance issues;

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

— a visible recognition of achievements in compliance management and outcomes;

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

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

— open and appropriate communication about compliance, internally and externally.

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

— the items above are implemented;

— interested parties (particularly personnel) believe that the items above have been implemented;

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

— corrective actions to address noncompliance are "owned" and actioned at all appropriate levels of the organization as required;

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

— personnel are enabled and encouraged to raise compliance concerns to the appropriate level of management, including top management and the governing body.

The organization should:

a) measure its culture of compliance;

b) seek input from all personnel to determine whether they perceive the governing body's, top management's and middle management's commitment to compliance;

c) establish action plans based on the results of the organization's compliance culture indicators.

A.5.1.3 Compliance governance

Compliance governance is founded on the following fundamental principles.

The compliance function has direct access to the governing body and top management. They can bypass others in the organization, should they need to, and directly communicate with the person or persons with the most authority to act. This is of direct benefit to the governing body and top management so they can exercise their duties. This access should be planned and systematic. For example, the compliance function can have a direct report to the CEO and a "dotted line" report to the audit committee, the chair or the entire board.

The compliance function should be independent and not conflicted by organizational structure or other elements. They are free to act without interference from line management.

The compliance function has authority. The compliance function is not a junior position that can be overruled or have reports or information altered by those above them in authority. The compliance function can direct other staff as necessary. The compliance function should have a "voice at the table" to advocate and raise any compliance concerns.

The compliance function is adequately resourced to support the organization to carry out the necessary work and responsibilities of the compliance management system without restrictions, including access to the technology to enable the compliance management system to be comprehensive and effectively support the organization in achieving its compliance objectives.

A.5.2 Compliance policy

The compliance policy establishes the overarching principles and commitment to action for an organization to achieve 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 be approved by the governing body.

The compliance policy should specify:

— the application and context of the compliance management 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 principles on which relationships with internal and external interested parties will be managed.

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

The compliance policy should be translated into other languages if necessary.

The compliance policy should be appropriate to the organization's compliance obligations that arise from its scope and activities.

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

a) specific international, regional or local obligations;

b) the organization's strategy, objectives, culture and governance approach;

c) the organization's structure;

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

e) adopted standards, codes, internal policies and procedures;

f) industry standards.

The compliance policy may comprise:

— a mission statement;

— a general policy statement;

— management strategies and allocation of responsibilities and resources;

— standard compliance procedures;

— audit, due diligence and compliance.

A.5.3 Roles, responsibilities and authorities

A.5.3.1 Governing body and top management

The active involvement of, and supervision by, a governing body is an integral part of an effective compliance management system. This helps ensure that personnel fully understand the organization's compliance policy and operational compliance 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 and visibly supporting compliance and the compliance management system.

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

Top management should encourage behaviour that creates and supports compliance and should not tolerate behaviour that compromises compliance.

Top management should ensure:

— the alignment of the organization's commitment to compliance with its values, objectives and strategy in order to position compliance appropriately;

— the encouragement of all employees to accept the importance of achieving the compliance objectives for which they are responsible or accountable;

— the creation of an environment where the reporting of noncompliance is encouraged and the reporting employee will be safe from retaliation;

— that compliance is incorporated into the broader organizational culture and culture change initiatives;

— the identification of noncompliance and prompt action to correct or address it;

— that operational objectives and targets do not compromise compliant behaviour.

Top management should review the performance of the compliance management system at planned intervals (e.g. quarterly or monthly) referencing KPIs and other key information to ensure that the compliance management system is achieving its objectives.

The effectiveness of a compliance management system requires a commitment by top management through the setting of standards and the exercise of reasonable oversight. Top management should be knowledgeable about the content and the operation of the compliance management system and should ensure that the organization has adequate processes for an effective compliance management system.

A.5.3.2 Compliance function

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. The compliance function works together with management.

Not all organizations will create a discrete compliance function; some will assign this function to an existing position or outsource that function. When outsourcing, organizations should consider not assigning the entire compliance function to third parties. Even if it outsources part of the function, it should consider keeping authority over it and oversee such functions.

In allocating responsibility for the compliance management system, consideration should be given to ensuring that the compliance function demonstrates:

— integrity and commitment to compliance;

— effective communication and influencing skills;

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

— relevant competence in designing, implementing and maintaining compliance management systems;

— assertiveness, business knowledge and experience to test and challenge;

— a strategic, proactive approach to compliance;

— enough time available to fulfil the needs of the role.

The compliance function should have authority, status and independence. Authority means that the compliance function is granted enough powers by the governing body and top management. Status means that other personnel are likely to listen to and respect his/her opinion. Independence means that the compliance function is, as far as possible, not personally involved in activities that are exposed to compliance risks.

The compliance function should be free from conflict of interest to fulfil its role.

A.5.3.3 Management

The responsibilities of top management 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.

The 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.

A.5.3.4 Personnel

Compliance with compliance obligations is expected of all personnel.

Personnel should ensure they are aware of their compliance responsibilities and effectively carry them out. They will be supported in this through elements of the compliance management system, such as training, policies and procedures, and the code of conduct.

Personnel should be proactive about contributing to insights and improvements that can assist in the performance of the compliance management system.

A.6 Planning

A.6.1 Actions to address risks and opportunities

Planning for the compliance management system is performed at a strategic level, versus the operation planning done for operational planning and control.

The purpose of planning is to anticipate potential scenarios and consequences and it is, as such, preventive. Based on the results of a compliance risk assessment, the organization should plan how to address undesired effects before they occur and how to benefit from favourable conditions or circumstances that can support the effectiveness of the compliance management system.

Planning should also include determining how to incorporate the actions deemed necessary or beneficial for the compliance management system into business activities and processes. The incorporation can either be achieved through objective setting, operational control or other specific clauses (e.g. resource provisions, competence). Measures for evaluating the effectiveness of the compliance management system should also be planned. This can include monitoring, measurement techniques, internal audit or management review.

A.6.2 Compliance objectives and planning to achieve them

Objectives should be specified in a way that allows outcomes to be measured.

An example of a compliance objective: to deliver compliance training to relevant personnel at least annually.

The actions required to achieve the objectives (i.e. “what”), an associated timeframe (i.e. “when”) and the person responsible (i.e. “who”) should be determined. The status and progress of objectives should be periodically monitored, recorded, assessed and updated as required.

A.7 Support

A.7.1 Resources

Resources include financial, human and technical 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.

A.7.2 Competence

A.7.2.1 General

The term “competence” means the ability to apply knowledge and skills to achieve intended results. Competence requires knowledge, experience and skills so that person can perform their function in an effective manner. The organization should determine for all personnel the expertise and knowledge necessary to fulfil their task so that the organization can provide its products and services to customers. The organization should establish evidence of competence (e.g. job descriptions, position statements), which can be considered when filling positions.

Measures (e.g. training) should be taken to ensure that existing competences are maintained and new ones are acquired. There should be adequate documentation of competences, as well as measures taken to maintain or acquire these competences.

A.7.2.2 Employment process

Prior to hiring personnel or promoting existing personnel, the organization should undertake due diligence, which can include reference or background checks.

A.7.2.3 Training

The governing body, management and personnel having 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 programme is to ensure that personnel 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 personnel to communicate previously unidentified compliance risks.

Education and training should be:

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

— sufficiently flexible to account for a range of techniques to accommodate the differing needs of organizations and personnel;

— designed, developed and delivered by experienced and qualified personnel;

— delivered in the local language where applicable;

— evaluated and assessed as to its effectiveness on a regular basis.

Interactive training can be the best form of training, if noncompliance can result in serious consequences.

The organization should provide training in the area where the misconduct has occurred.

Compliance retraining should be considered whenever there is:

— a change of position or responsibilities;

— a change in internal policies, processes and procedures;

— a change in the organizational structure;

— a change in the compliance obligations, especially in legal requirements and requirements of interested parties;

— a change in activities, products or services;

— an issue arising from monitoring, auditing, reviews, complaints and noncompliance, including interested party feedback.

A.7.3 Awareness

Awareness involves ensuring that compliance policies are made accessible and available to all personnel and are understood.

Raising compliance awareness can be achieved by methods such as, but not limited to:

— training (face to face or online);

— communication from top management;

— easy-to-follow and readily accessible reference materials;

— regular updates on compliance issues.

Communicating commitment to compliance:

— builds awareness and motivates personnel to embrace the compliance management system;

— encourages employees to make suggestions that facilitate continual improvement in compliance performance.

A.7.4 Communication

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

Interested parties can include regulatory bodies, customers, contractors, suppliers, investors, emergency services, non-governmental organizations and neighbours.

The organization should allocate the appropriate resources and people with the relevant knowledge to coordinate and facilitate regulatory interaction.

Methods of communication may include websites and emails, 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.

Communications should adhere to the principles of transparency, appropriateness, credibility, responsiveness, accessibility and clarity.

A.7.5 Documented information

A.7.5.1 General

Documented information can include:

— the organization's compliance policy and procedures;

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

— the allocation of roles and responsibilities for compliance;

— a register of relevant compliance obligations;

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

— a register of noncompliances, near misses and investigations;

— annual compliance plans;

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

— the audit process, audit schedule and associated audit records.

Documented information can include matters relating to regulatory reporting requirements. Documented information may comprise all sorts of media (digital and non-digital).

A.7.5.2 Creating and updating documented information

Documented information should be updated to reflected internal and external changes to ensure that they are current and up to date.

A.7.5.3 Control of documented information

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

A.8 Operation

A.8.1 Operational planning and control

A well-designed compliance management system comprises measures (e.g. policies, processes, procedures) that give both content and effect to a compliance culture. They address and aim to reduce risks identified as part of the compliance risk assessment process.

A basic element of operational control is a code of conduct that sets forth, among other things, the organization's full commitment to relevant compliance obligations. A code of conduct should be applicable to all personnel and be accessible to them. Based upon and derived from the code of conduct, compliance measures should be incorporated into the day-to-day operations of the organization to foster a culture of compliance.

Operational controls are required for situations related to business processes where an absence of such controls can lead to deviations to the compliance policy or a breach of compliance obligations. These situations can be related to all business situations, activities or processes (e.g. production, installation, servicing, maintaining) or to contractors, suppliers or vendors.

The degree of control can vary depending upon several factors such as the importance or complexity of the functions performed, the potential consequences of noncompliance or the technical support involved or available.

When operational controls fail, actions are necessary to address any undesirable results or effects.

If there is any use of third parties or outsourced processes in the organization's activities, the organization should undertake effective due diligence to ensure that its standards and commitment to compliance will not be lowered. An example of third parties relates to the provision of products and services and distribution of products. The organization should ensure that appropriate service-level agreements (SLAs) specifying compliance obligations for the service provider are concluded.

A well-designed outsource process considers the following:

— initial and ongoing due diligence;

— implement appropriate controls;

— undertaking ongoing monitoring;

— an appropriate review of legal/contractual agreements;

— consideration of SLAs;

— using third parties certified to this document.

When making a contract with third parties, the organization should implement controls to ensure that the procurement, operational, commercial and other non-financial aspects of its activities are being properly managed. Depending on the size of the organization and transaction, the procurement, operational, commercial and other non-financial controls implemented by an organization can reduce compliance risks.

A.8.2 Establishing controls and procedures

Effective controls are needed to ensure that the organization's compliance obligations are met, and that noncompliances are prevented, detected and corrected. Controls should be designed with enough 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.

Controls can include:

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

— systems and exception reports;

— approvals;

— the segregation of incompatible roles and responsibilities;

— automated processes;

— annual compliance plans;

— personnel 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 the expected behaviour of employees (standards and values, codes of conduct).

In developing procedures to support compliance management, consideration should be given to:

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

— consistency with other review and control functions in the organization;

— ongoing monitoring and measurement;

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

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

A.8.3 Raising concerns

Where appropriate, escalation should be to top management and the governing body, including relevant committees.

Even when not required by local regulation, organizations should consider developing a whistleblower mechanism to allow for anonymity or confidentiality, whereby the organization's employees and agents can report or seek guidance of noncompliance without fear of retaliation.

For more guidance on whistleblowing management systems see ISO/DIS 37002.[1)]

A.8.4 Investigation process

A characteristic of an effective compliance management system is a well-functioning mechanism for the timely and thorough investigation of any allegations or suspicions of misconduct by the organization, its personnel or relevant third parties. This includes the documentation of the organization's response, including any disciplinary or remediation measures taken, and revisions of the compliance management system considering lessons learned.

An effective investigation mechanism identifies the root causes of misconduct, vulnerabilities of the compliance management system and accountability lapses, including among managers, top management

1) Under preparation. Stage at the time of publication: ISO/DIS 37002:2020.

and the governing body. A thoughtful root-cause analysis addresses the extent and pervasiveness of the noncompliance, the number and level of the personnel involved, and the seriousness, duration and frequency of the noncompliance.

Organizations should make sure that the investigations are fair and independent. They should consider, when appropriate, creating independent committees to oversee the investigation and guarantee their completeness and independence.

The organization should establish a reporting mechanism on investigations, including the level up to which the findings of investigations are to be reported.

NOTE Organizations are sometimes required by law to report noncompliance. In such cases, regulatory authorities are informed in accordance with the applicable regulations, or as otherwise agreed.

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

A.9 Performance evaluation

A.9.1 Monitoring, measurement, analysis and evaluation

A.9.1.1 General

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;

— reviews of business strategy against compliance risks to enable approriate updating.

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;

— establishment of leading and lagging indicators.

A.9.1.2 Sources of feedback on compliance performance

Sources include:

— personnel (e.g. through whistleblowing facilities, helplines, feedback, suggestion boxes);

— customers (e.g. through a complaint handling system);

— third parties;

— suppliers;

— contractors;

— regulators;

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

Feedback on compliance performance can include:

— compliance issues;

— noncompliances and compliance concerns;

— emerging compliance issues;

— ongoing regulatory and organizational changes;

— comments on compliance effectiveness and performance.

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.

Information collection can include:

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

— information gained through hotlines, complaints and other feedback, including whistleblowing;

— 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;

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

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

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

Information classification criteria can include:

— source;

— department;

— noncompliance description;

— obligation references;

— indicators;

— severity;

— actual or potential impact.

A.9.1.3 Development of indicators

This process should take into account the results of the assessment of compliance risks 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 programmes being implemented.

Indicators can include:

— the percentage of employees trained effectively;

— the frequency of contacts by regulators;

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

Reactive indicators can include:

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

— the consequence of noncompliance, which can include a valuation of the 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.

Predictive indicators can include:

— risks of noncompliances measured as the potential loss/gain of objectives (revenue, health and safety, reputation, etc.) over time;

— noncompliance trends (the expected compliance rate based on past trends).

A.9.1.4 Compliance reporting

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 can indicate a 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 a failure becoming a systemic problem.

Compliance reports should include:

— any matters that the organization are required to notify to any regulatory authority;

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

— measurement of compliance performance, including noncompliance and continual improvement;

— the number and details of possible noncompliances and a subsequent analysis of them;

— corrective actions undertaken;

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

— contacts, and developments in relationships, with regulators;

— results from audits, as well as monitoring activities;

— monitoring the complete execution of action plans, especially those derived from audit reports or regulator requirements, or both.

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

A.9.1.5 Record-keeping

Record-keeping should include recording and classifying compliance issues 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:

— information on compliance performance, including compliance reports;

— details of noncompliance and corrective actions;

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

A.9.2 Internal audit

Audit functions, whether internal or external, should be free of conflicts of interest and independent in order to fulfil their role.

See ISO 19011 for information on how to conduct an audit of a management system.

A.9.3 Management review

Management review should also include recommendations on:

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

— changes to compliance processes to ensure the effective integration with operational practices and systems;

— areas to be monitored for potential future noncompliance;

— corrective actions with respect to noncompliance;

— gaps or lack in current compliance systems and longer-term continual improvement initiatives;

— the recognition of exemplary compliance behaviour within the organization.

A copy of the documented results and any recommendations in the management review should be provided to the governing body.

A.10 Improvement

A.10.1 Continual improvement

The effectiveness of a compliance management system is characterized by the fact that it has the capacity to continually improve and evolve. The organization's internal and external environment and business changes over time, as do the nature of its customers and applicable compliance obligations.

The adequacy and effectiveness of the compliance management system should be assessed on a continual and regular basis through several methods, e.g. reviews by internal audits.

The organization should establish measures to review its compliance management system and to ensure that it remains current and fit for purpose. When determining the extent and timescale of actions that support continual improvement, the organization should consider its context, economic factors and other relevant circumstances.

Some organizations survey employees to measure the compliance culture and evaluate the strength of controls. Further sources of information for continual improvement can be the results of customer surveys, reports raising concern, regular monitoring, periodic audits or management reviews.

The organization should consider the results and outputs of such assessments to determine if there is a need or opportunity to change the compliance management system.

In order to help ensure that the integrity of the compliance management system and its effectiveness is retained, changes in individual elements of the management system should take into account the dependency and the impact of such changes on the effectiveness of the management system as a whole.

When making changes to the compliance management system, the organization should consider the implications these changes have for the compliance management system, its operations, the availability of resources, the compliance risk assessments, the organization's compliance obligations and its continual improvement processes.

A.10.2 Nonconformity and corrective action

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 a noncompliance.

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

— assessing product and service performance;

— improving or redesigning products and services;

— changing organizational practices and procedures;

— retraining employees;

— reassessing the need to inform interested parties;

— providing an early warning of a potential noncompliance;

— redesigning or reviewing controls;

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

— communicating facts surrounding the noncompliance and the organization's position concerning the noncompliance.

The organization should identify the root causes of not following policies or procedures, or both, that contributed to the misconduct and update the policy and procedure based on the lessons learned.

Bibliography

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

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

[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/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO 31000, *Risk management — Guidelines*

[9] IEC 31010, *Risk management — Risk assessment techniques*

[10] ISO 37001, *Anti-bribery management systems — Requirements with guidance for use*

[11] ISO 37002[2)], *Whistleblowing management systems — Guidelines*

[12] ISO Guide 73, *Risk management — Vocabulary*

2) Under preparation. Stage at the time of publication: ISO/DIS 37002:2020.

ICS 03.100.01; 03.100.02; 03.100.70

Price based on 40 pages