Foreword

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

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

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 309 *Governance of organizations*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

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

Good governance is the foundation of every effective compliance management system. The governing body of an organization assures the compliance function's independence and authority, its direct access to leadership at all levels and the required resources.

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

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

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

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

This document specifies requirements as well as provides guidance on compliance management systems and recommended practices. Both the requirements and the guidance in this document are intended to be adaptable, and the implementation of this can differ depending on the size and level of maturity of an organization's compliance management system and on the context, nature and complexity of the organization's activities, including its compliance policy and objectives.

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

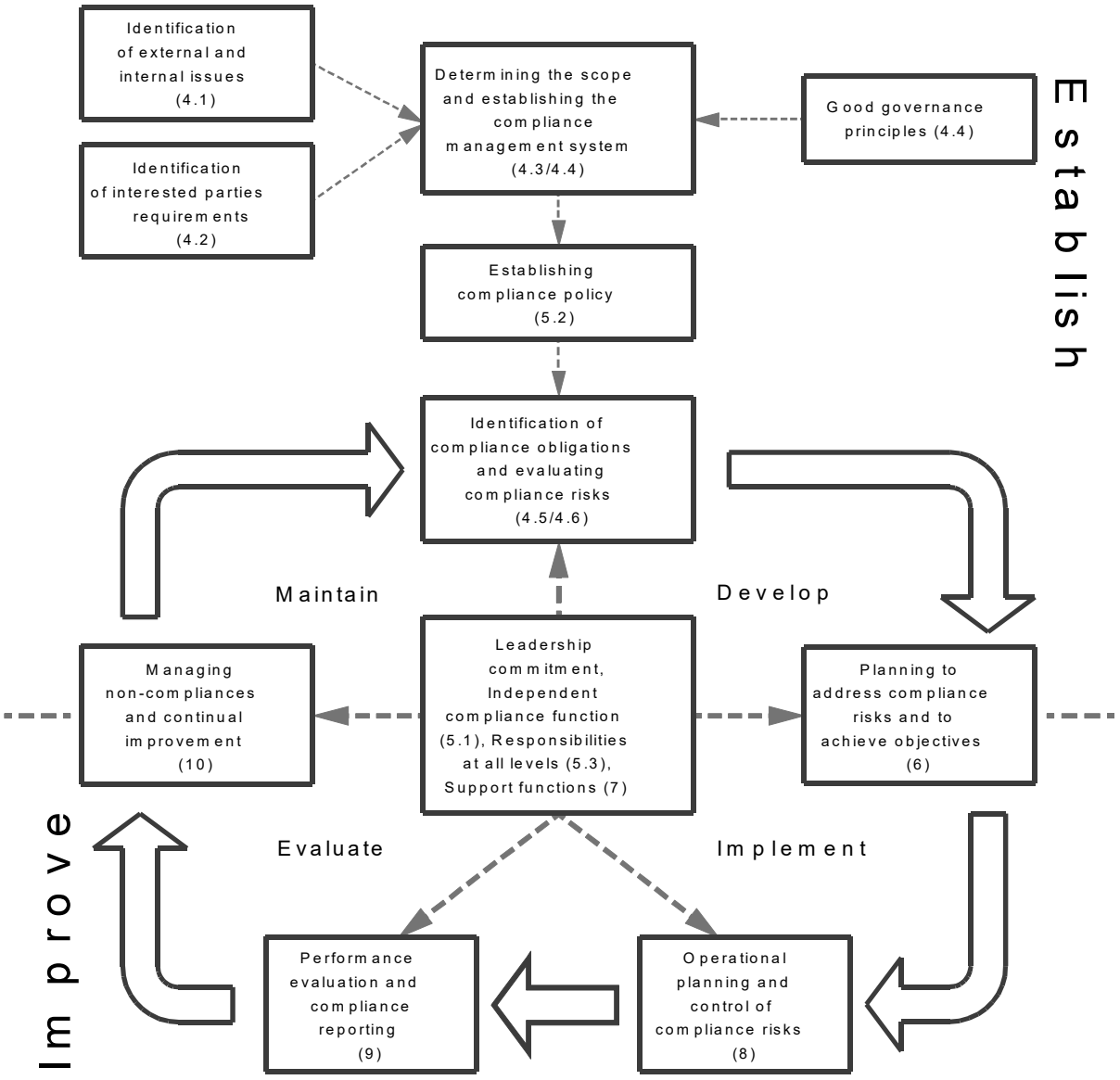

Figure 1 — Flowchart of a compliance management system

This document has adopted the "high-level structure" (i.e. clause sequence, common text and common terminology) developed by ISO to improve alignment among its International Standards for management systems.

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

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

Compliance management systems — Requirements with guidance for use

1 Scope

This document specifies requirements and gives 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. It is based on the principles of good governance, proportionality, transparency and sustainability.

2 Normative references

There are no normative references in this document.

3 Terms and definition

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* (3.10)

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

3.2
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.1) that can affect, be affected by, or perceive 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* (3.7) 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
governing body
person(s) that has the ultimate responsibility and authority for an *organization's* (3.1) activities, governance and policies 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, board of directors, committees of the board, supervisory board, trustees or overseers.

3.5
personnel
individuals in a relationship recognized as an employment relationship in national law or practice

3.6
compliance function
person(s) with responsibility and authority for the operation of the *compliance* (3.15) *management system* (3.7)

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

3.7
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.9) and *objectives* (3.10) and *processes* (3.11) to achieve those objectives

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

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

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

3.8
effectiveness
extent to which planned activities are realized and planned results achieved

3.9
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3) and/or its governing body

3.10
objective
result to be achieved