![SIST logo]

SLOVENSKI STANDARD
oSIST ISO/DIS 37301:2021

01-januar-2021

Sistemi za upravljanje skladnosti - Zahteve z napotki za uporabo

Compliance management systems - Requirements with guidance for use

Systèmes de management de la conformité - Exigences et recommandations pour la mise en oeuvre

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: **ISO/DIS 37301**

ICS:

03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general
03.100.70	Sistemi vodenja	Management systems

oSIST ISO/DIS 37301:2021 **en,fr,de**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

DRAFT INTERNATIONAL STANDARD
ISO/DIS 37301

ISO/TC **309**

Secretariat: **BSI**

Voting begins on:
2020-03-13

Voting terminates on:
2020-06-05

Compliance management systems — Requirements with guidance for use

ICS: 03.100.01; 03.100.02; 03.100.70

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 37301:2020(E)

© ISO 2020

ISO/DIS 37301:2020(E)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

This document cancels and replaces ISO 19600:2014-10.

In this International Standard, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates permission:

— "can" indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirements.

ISO/DIS 37301:2020(E)

Introduction

Organizations that aim to be successful in the long term need to establish and maintain a culture of integrity and compliance, considering 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 ongoing process and the outcome of an organization meeting its obligations. Compliance 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 other management processes and its operational requirements and procedures.

An effective, organization-wide compliance management system enables an organization to demonstrate its commitment to comply 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 organization's compliance obligations. Integrity and effective compliance are therefore key elements of good and diligent management. Compliance also contributes to the socially responsible behaviour of organizations.

One of the objectives of this document is to assist organizations to develop and spread a positive culture of compliance, considering that an effective and sound management of compliance-related risks should be regarded as an opportunity to pursue and take, due to the several benefits that it provides to the organization.

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 and objectives.

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.
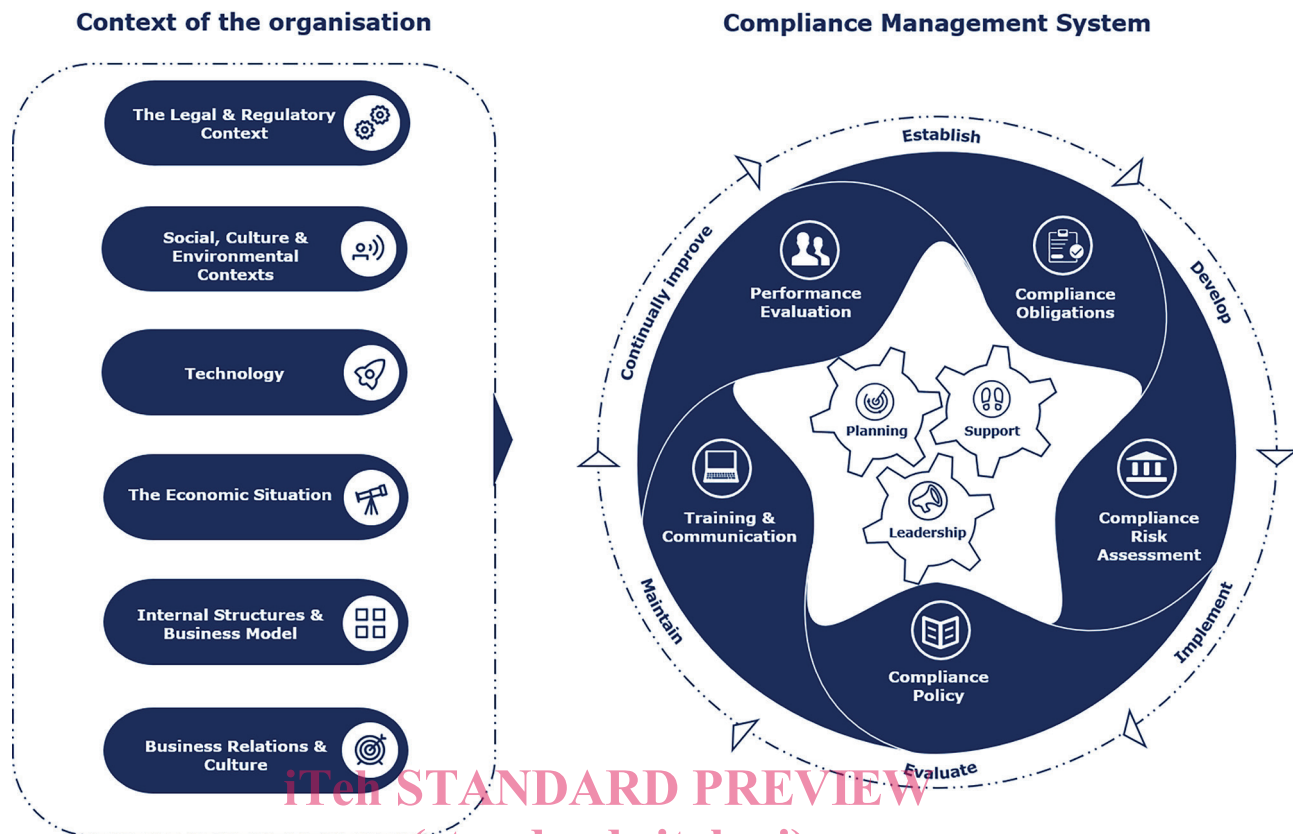
Figure 1 —

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 which 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* (3.8)

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

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

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

3.4
management system
set of interrelated or interacting elements of an *organization* ([3.1](#)) to establish *policies* ([3.7](#)) and *objectives* ([3.8](#)) and *processes* ([3.12](#)) 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.

3.5
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.

3.6
effectiveness
extent to which planned activities are realized and planned results achieved

3.7
policy

intentions and direction of an *organization* ([3.1](#)) as formally expressed by its *top management* ([3.5](#)) and/or its governing body ([3.22](#))

3.8
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 financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* ([3.12](#)).

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

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

3.9
risk
effect of uncertainty

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.

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
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* ([3.12](#));

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

— evidence of results achieved (records).

3.12
process
set of interrelated or interacting activities which transforms inputs into outputs

3.13
performance
measurable result

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

Note 2 to entry: Performance can relate to managing activities, *processes* ([3.12](#)), products (including services), systems or *organizations* ([3.1](#))

3.14
outsource (verb)
make an arrangement where an external *organization* ([3.1](#)) performs part of an organization's function or *process* ([3.11](#))

Note 1 to entry: An external organization is outside the scope of the *management system* ([3.4](#)), although the outsourced function or process is within the scope.

3.15
monitoring
determining the status of a system, a *process* ([3.12](#)) or an activity

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

3.16
measurement
process ([3.12](#)) to determine a value

3.17
audit
systematic, independent and documented *process* ([3.12](#)) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

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

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

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

ISO/DIS 37301:2020(E)

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.

**3.18
conformity**
fulfilment of a *requirement* ([3.3](#))

**3.19
nonconformity**
non-fulfilment of a *requirement* ([3.3](#))

Note 1 to entry: A nonconformity is not necessarily a *noncompliance* ([3.28](#)).

**3.20
corrective action**
action to eliminate the cause(s) of a *nonconformity* ([3.19](#)) or a *noncompliance* ([3.28](#)) and to prevent recurrence

**3.21
continual improvement**
recurring activity to enhance *performance* ([3.13](#))

**3.22
governing body**
person or group of persons that has the ultimate responsibility and authority for an *organization's* ([3.1](#)) activities, governance and policies and to which *top management* ([3.5](#)) 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, or trustees.

**3.23
personnel**
individuals in a relationship recognized as work relationship in national law or practice, or in any contractual relationship which depends on its activity from the *organization* ([3.1](#))

**3.24
compliance function**
person or group of persons with responsibility and authority for the operation of the *compliance* ([3.27](#)) *management system* ([3.4](#))

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

**3.25
compliance risk**
likelihood of occurrence and the consequences of *noncompliance* ([3.17](#)) with the organization's *compliance obligations* ([3.26](#))

**3.26
compliance obligation**
requirements ([3.3](#)) that an *organization* ([3.1](#)) mandatorily has to comply with as well as those that an *organization* ([3.1](#)) voluntarily chooses to comply with

**3.27
compliance**
the outcome of meeting all the organization's *compliance obligations* ([3.26](#))

3.28
noncompliance
non-fulfilment of a *compliance obligation* (3.26)

3.29
compliance culture
values, ethics and beliefs that exist throughout an *organization* (3.1) and interact with the organization's structures and control systems to produce behavioural norms that are conducive to *compliance* (3.27) outcomes

3.30
conduct
an organisation's behaviours and practices that impact outcomes for customers, employees, suppliers, markets and communities

3.32
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

3.33
procedure
specified way to carry out an activity or *process* (3.12)

[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 outcome(s) of its compliance management system.

For this purpose, the organization shall consider a broad range of issues, including:

— the legal and regulatory context;

— social, cultural, and environmental contexts;

— technology;

— the economic situation;

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

— 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 current 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.