INTERNATIONAL STANDARD

ISO 37301

First edition
2021-04

Compliance management systems — Requirements with guidance for use

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

SIST Preview
(https://ecommerce.sist.si)

ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

Reference number
ISO 37301:2021(E)

© ISO 2021

SIST Preview
(https://ecommerce.sist.si)

ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

 © ISO 2021 – All rights reserved

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Context of the organization **5**
4.1 Understanding the organization and its context 5
4.2 Understanding the needs and expectations of interested parties 5
4.3 Determining the scope of the compliance management system 5
4.4 Compliance management system 6
4.5 Compliance obligations 6
4.6 Compliance risk assessment 6
5 Leadership **6**
5.1 Leadership and commitment 6
5.1.1 Governing body and top management 6
5.1.2 Compliance culture 7
5.1.3 Compliance governance 7
5.2 Compliance policy 8
5.3 Roles, responsibilities and authorities 8
5.3.1 Governing body and top management 8
5.3.2 Compliance function 9
5.3.3 Management 10
5.3.4 Personnel 10
6 Planning **10**
6.1 Actions to address risks and opportunities 10
6.2 Compliance objectives and planning to achieve them 11
6.3 Planning of changes 11
7 Support **12**
7.1 Resources 12
7.2 Competence 12
7.2.1 General 12
7.2.2 Employment process 12
7.2.3 Training 12
7.3 Awareness 13
7.4 Communication 13
7.5 Documented information 14
7.5.1 General 14
7.5.2 Creating and updating documented information 14
7.5.3 Control of documented information 14
8 Operation **15**
8.1 Operational planning and control 15
8.2 Establishing controls and procedures 15
8.3 Raising concerns 15
8.4 Investigation processes 15
9 Performance evaluation **16**
9.1 Monitoring, measurement, analysis and evaluation 16
9.1.1 General 16
9.1.2 Sources of feedback on compliance performance 16
9.1.3 Development of indicators 16
9.1.4 Compliance reporting 16
9.1.5 Record-keeping 17

SIST Preview
(https://ecommerce.sist.si)
ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

© ISO 2021 – All rights reserved

9.2 Internal audit 17
9.2.1 General 17
9.2.2 Internal audit programme 17
9.3 Management review 17
9.3.1 General 17
9.3.2 Management review inputs 18
9.3.3 Management review results 18
10 Improvement 18
10.1 Continual improvement 18
10.2 Nonconformity and corrective action 19
Annex A (informative) **Guidance for the use of this document 20**
Bibliography 40

SIST Preview
(https://ecommerce.sist.si)
ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

 © ISO 2021 – All rights reserved

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.

SIST Preview
(https://standards.iteh.ai)

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

This first edition of ISO 37301 cancels and replaces ISO 19600:2014, which has been technically revised.

ISO 37301:2021
https://standards.iteh.ai/catalog/standards/iso/d0bad0df-5256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

The main changes compared to ISO 19600:2014 are as follows:

— this document now contains requirements with additional guidance for use based on those requirements;

— this document follows ISO's requirements for a harmonized structure for management system standards.

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.

© ISO 2021 – All rights reserved

Introduction

Organizations that aim to be successful in the long term need to establish and maintain a culture of compliance, considering the needs and expectations of interested parties. Compliance is 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 that 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, regulatory requirements, industry codes and organizational standards, as well as standards of good governance, generally accepted best practices, ethics and community expectations.

An organization's approach to compliance is shaped by the leadership applying core values and generally accepted good 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.

SIST Preview
(https://ecommerce.sist.si)

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 such as:

— improving business opportunities and sustainability;

— protecting and enhancing an organization's reputation and credibility;

— taking into account expectations of interested parties;

— demonstrating an organization's commitment to managing its compliance risks effectively and efficiently;

— increasing the confidence of third parties in the organization's capacity to achieve sustained success;

— minimizing the risk of a contravention occurring with the attendant costs and reputational damage.

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 implementation 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.

© ISO 2021 – All rights reserved

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 provides an overview on common elements of a compliance management system.

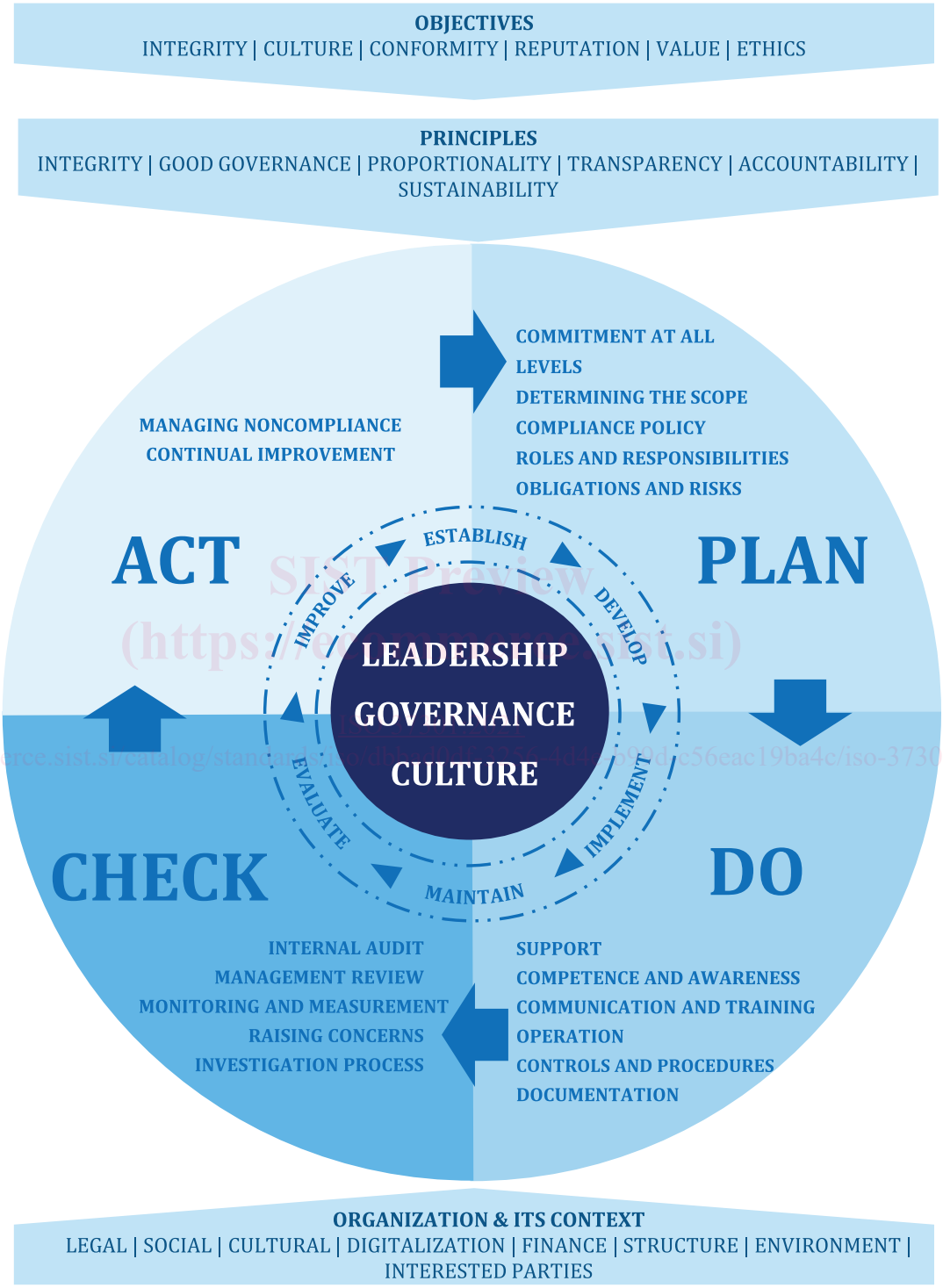

Figure 1 — Elements of a compliance management system

SIST Preview
(https://ecommerce.sist.si)
https://ecommerce.sist.si/catalog/standards/iso/dbbcd0df-3256-4d4f-a690-dfc56eac19ba4c/iso-37301-2021

© ISO 2021 – All rights reserved

In this document, 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.

Annex A provides guidance for the use of this document.

SIST Preview
(https://ecommerce.sist.si)
ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

© ISO 2021 – All rights reserved

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

SIST Preview
(https://ecommerce.sist.si)
ISO 37301:2021
https://ecommerce.sist.si/catalog/sist/dbb1d9df-3256-4d4a-b99d-c56eac19ba4c/iso-37301-2021

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.

© ISO 2021 – All rights reserved

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* (3.21).

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* (3.26) objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

SIST Preview
(https://ecommerce.sist.si)

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.

ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

3.7
risk
effect of uncertainty on *objectives* (3.6)

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

© ISO 2021 – All rights reserved

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.

SIST Preview
(https://ecommerce.sist.si)
ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-5256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

© ISO 2021 – All rights reserved

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 the 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)

SIST Preview
(standards.iteh.ai)
ISO 37301:2021

© ISO 2021 – All rights reserved

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, including, but 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.

SIST Preview
(https://ecommerce.sist.si)
ISO 37301:2021
https://ecommerce.sist.si/catalog/standards/iso/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-37301-2021

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.

© ISO 2021 – All rights reserved

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, 4.5 and 4.6.

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;

SIST Preview
(https://standards.iteh.ai)
ISO 37301:2021

 © ISO 2021 – All rights reserved