
Compliance management systems — Requirements with guidance for use

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



This document is a preview generated by EKO



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

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

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

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*.

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

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.

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.

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.

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

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.

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.