
Compliance management systems — Guidelines

Systèmes de management de la conformité — Lignes directrices



Reference number
ISO 19600:2014(E)



COPYRIGHT PROTECTED DOCUMENT

© ISO 2014

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definition	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 and principles of good governance	6
4.5 Compliance obligations	6
4.6 Identification, analysis and evaluation of compliance risks	7
5 Leadership	8
5.1 Leadership and commitment	8
5.2 Compliance policy	9
5.3 Organizational roles, responsibilities and authorities	10
6 Planning	13
6.1 Actions to address compliance risks	13
6.2 Compliance objectives and planning to achieve them	14
7 Support	14
7.1 Resources	14
7.2 Competence and training	14
7.3 Awareness	16
7.4 Communication	17
7.5 Documented information	18
8 Operation	19
8.1 Operational planning and control	19
8.2 Establishing controls and procedures	19
8.3 Outsourced processes	20
9 Performance evaluation	21
9.1 Monitoring, measurement, analysis and evaluation	21
9.2 Audit	25
9.3 Management review	25
10 Improvement	26
10.1 Nonconformity, noncompliance and corrective action	26
10.2 Continual improvement	27
Bibliography	28

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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is Project Committee ISO/PC 271, *Compliance management systems*.

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 stakeholders. 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.

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 ideally 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, the 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 International Standard 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 International Standard does not specify requirements, but provides guidance on compliance management systems and recommended practices. The guidance in this International Standard is intended to be adaptable, and the use of this guidance 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").