



Compliance management systems— Guidelines



This Australian Standard® was prepared by Committee QR-014, Compliance Systems. It was approved on behalf of the Council of Standards Australia on 2 June 2015. This Standard was published on 22 June 2015.

The following are represented on Committee QR-014:

- Australian Chamber of Commerce and Industry
 - Australian Industry Group
 - Australian Institute of Company Directors
 - Australian National Retailers Association
 - Australian Prudential Regulation Authority
 - Consumers Federation of Australia
 - Council of Small Business Organisations of Australia
 - GRC Institute
 - Joint Accreditation System of Australia and New Zealand
 - Law Council of Australia
 - Society of Consumer Affairs Professionals
-

This Standard was issued in draft form for comment as DR AS/NZS ISO 19600:2015.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

Compliance management systems— Guidelines

Originated as AS 3806—1998.
Revised and redesignated as AS ISO 19600:2015.

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 76035 089 5

PREFACE

This Standard was prepared by the Standards Australia Committee QR-014, Compliance Systems, to supersede AS 3806—2006, *Compliance programs*.

The objective of this Standard is to provide guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization.

This Standard is identical with, and has been reproduced from ISO 19600:2014, *Compliance management systems—Guidelines*.

As this Standard is reproduced from an International Standard, the following applies:

- (a) In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- (b) A full point substitutes for a comma when referring to a decimal marker.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO will 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.

CONTENTS

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

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").

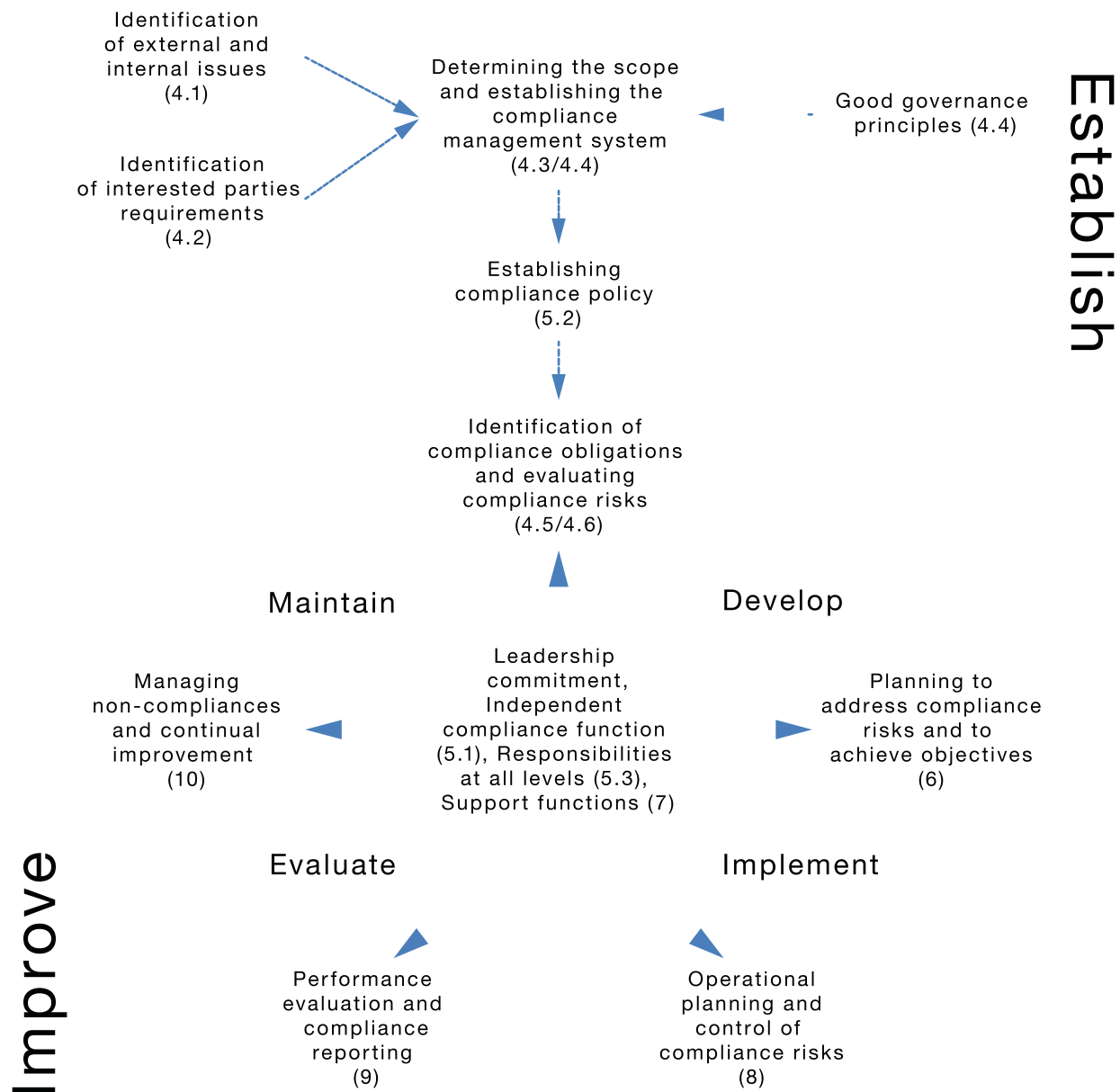


Figure 1 — Flowchart of a compliance management system

This International Standard 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. In addition to its generic guidance on a compliance management system, this International Standard also provides a framework to assist in the implementation of specific compliance-related requirements in any management system.

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

This International Standard 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.

This International Standard can be combined with existing management system standards (e.g. ISO 9001, ISO 14001, ISO 22000) and generic guidelines (e.g. ISO 31000, ISO 26000).

NOTES

AUSTRALIAN STANDARD

Compliance management systems—Guidelines**1 Scope**

This International Standard provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization.

The guidelines on compliance management systems are applicable to all types of organizations. The extent of the application of these guidelines depends on the size, structure, nature and complexity of the organization. This International Standard is based on the principles of good governance, proportionality, transparency and sustainability.

2 Normative references

There are no normative references.

3 Terms and definition

For the purpose of this document, the following terms and definitions apply.

3.1**organization**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.9)

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 themselves 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.

3.4**governing body**

person or group of people that governs an *organization* (3.1), sets directions and holds *top management* (3.3) to account

3.5**employee**

individual in a relationship recognized as an employment relationship in national law or practice

3.6

compliance function

person(s) with responsibility for *compliance* (3.17) management

Note 1 to entry: Preferably one individual will be assigned overall responsibility for *compliance* (3.17) management

3.7

management system

set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.8) and *objectives* (3.9) and *processes* (3.10) 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, operation, etc.

Note 3 to entry: The scope of a management system may 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

policy

intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.7)

3.9

objective

result to be achieved

Note 1 to entry: An objective can be strategic, tactical and/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* (3.10)).

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.

3.10

process

set of interrelated or interacting activities which transforms inputs into outputs

3.11

risk

effect of uncertainty on *objectives* (3.9)

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 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), 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 73:2009, 3.6.1.1) of occurrence.

3.12

compliance risk

effect of uncertainty on compliance *objectives* (3.9)

Note 1 to entry: Compliance risk can be characterized by the likelihood of occurrence and the consequences of *noncompliance* (3.18) with the organization's *compliance obligations* (3.16).

3.13**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, for example in documented information.

3.14**compliance requirement**

requirement (3.13) that an organization (3.1) has to comply with

3.15**compliance commitment**

requirement (3.13) that an organization (3.1) chooses to comply with

3.16**compliance obligation**

compliance requirement (3.14) or compliance commitment (3.15)

3.17**compliance**

meeting all the organization's *compliance obligations (3.16)*

Note 1 to entry: Compliance is made sustained by embedding it in the culture of an *organization (3.1)* and in the behaviour and attitude of people working for it.

3.18**noncompliance**

non-fulfilment of a *compliance obligation (3.16)*

Note 1 to entry: Noncompliance can be a single or a multiple event and may or may not be the result of a *nonconformity (3.33)*.

3.19**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 (3.17)* outcomes

3.20**code**

statement of practice developed internally or by an international, national or industry body or other *organization (3.1)*

Note 1 to entry: The code may be mandatory or voluntary.

3.21**organizational and industry standards**

documented *codes (3.20)*, good practices, charters, technical and industry standards deemed by an *organization (3.1)* to be relevant

3.22**regulatory authority**

organization (3.1) responsible for regulating or enforcing *compliance (3.17)* with legislative and other *requirements (3.13)*

3.23**competence**

ability to apply knowledge and skills to achieve intended results

3.24**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* (3.7), including related *processes* (3.10);
- information created in order for the organization to operate (documentation);
- evidence of results achieved (records).

3.25**procedure**

specified way to carry out an activity or *process* (3.10)

3.26**performance**

measurable result

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

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.10), products (including services), systems or *organizations* (3.1).

3.27**continual improvement**

recurring activity or *process* (3.10) to enhance *performance* (3.26)

3.28**outsource** (verb)

make an arrangement where an external *organization* (3.1) performs part of an organization's function or *process* (3.10)

Note 1 to entry: An external organization is outside the *management system* (3.7), although the outsourced function or process is within the scope.

3.29**monitoring**

determining the status of a system, a *process* (3.10) or an activity

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

Note 2 to entry: Monitoring is not a once-only activity, but a process of regularly or continuously observing a situation.

3.30**measurement**

process (3.10) to determine a value

3.31**audit**

systematic, independent and documented *process* (3.10) 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: "Audit evidence" and "audit criteria" are defined in ISO 19011.

Note 3 to entry: Independence can be demonstrated by the freedom from responsibility for the activity being audited or freedom from bias and conflict of interest.

3.32

conformity

fulfilment of a management system *requirement* ([3.13](#))

3.33

nonconformity

non-fulfilment of a management system *requirement* ([3.13](#))

Note 1 to entry: A nonconformity is not necessarily a *noncompliance* ([3.18](#)).

3.34

correction

action to eliminate a detected *nonconformity* ([3.33](#)) or a *noncompliance* ([3.18](#))

3.35

corrective action

action to eliminate the cause of a *nonconformity* ([3.33](#)) or a *noncompliance* ([3.18](#)) and to prevent recurrence

4 Context of the organization

4.1 Understanding the organization and its context

The organization should determine external and internal issues, such as those related to compliance risks, that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its compliance management system. In doing so, the organization should consider a broad range of external and internal aspects, such as the regulatory, social and cultural contexts, the economic situation and the internal policies, procedures, processes and resources.

4.2 Understanding the needs and expectations of interested parties

The organization should determine:

- the interested parties that are relevant to the compliance management system;
- the requirements of these interested parties.

4.3 Determining the scope of the compliance management system

The organization should 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 geographical and/or organizational boundaries to which the compliance management system will apply, especially if the organization is a part of a larger organization at a given location.

When determining this scope, the organization should consider:

- the external and internal issues referred to in [4.1](#);
- the requirements referred to in [4.2](#) and [4.5.1](#).

The scope should be readily available as documented information.