NORME INTERNATIONALE

**ISO 19600**

Première édition
2014-12-15

# Systèmes de management de la compliance — Lignes directrices

*Compliance management systems — Guidelines*

Numéro de référence
ISO 19600:2014(F)

© ISO 2014



## DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2014

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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

Publié en Suisse

# Sommaire

Page

**Avant-propos** ..... **v**

**Introduction** ..... **vi**

**1 Domaine d'application** ..... **1**

**2 Références normatives** ..... **1**

**3 Termes et définitions** ..... **1**

**4 Contexte de l'organisme** ..... **5**
4.1 Connaissance de l'organisme et contexte ..... 5
4.2 Compréhension des besoins et des attentes des parties intéressées ..... 5
4.3 Détermination du périmètre du système de management de la compliance ..... 6
4.4 Système de management de la compliance et principes de bonne gouvernance ..... 6
4.5 Obligations de compliance ..... 6
4.5.1 Identification des obligations de compliance ..... 6
4.5.2 Tenue à jour des obligations de compliance ..... 7
4.6 Identification, analyse et évaluation des risques liés à la compliance ..... 7

**5 Leadership** ..... **8**
5.1 Leadership et engagement ..... 8
5.2 Politique de compliance ..... 9
5.2.1 Généralités ..... 9
5.2.2 Développement ..... 10
5.3 Rôles, responsabilités et autorités au sein de l'organisme ..... 10
5.3.1 Généralités ..... 10
5.3.2 Attribution des responsabilités pour la compliance au sein de l'organisme ..... 11
5.3.3 Rôle et responsabilité de l'organe directeur et de la direction ..... 11
5.3.4 Fonction en charge de la compliance ..... 12
5.3.5 Responsabilités du personnel d'encadrement ..... 13
5.3.6 Responsabilité des employés ..... 14

**6 Planification** ..... **14**
6.1 Actions pour traiter les risques liés à la compliance ..... 14
6.2 Objectifs de compliance et planification pour les atteindre ..... 14

**7 Soutien** ..... **15**
7.1 Ressources ..... 15
7.2 Compétences et formation ..... 15
7.2.1 Compétences ..... 15
7.2.2 Formation ..... 16
7.3 Sensibilisation ..... 17
7.3.1 Généralités ..... 17
7.3.2 Comportements ..... 17
7.4 Communication ..... 19
7.4.1 Généralités ..... 19
7.4.2 Communication interne ..... 19
7.4.3 Communication externe ..... 19
7.5 Informations documentées ..... 19
7.5.1 Généralités ..... 19
7.5.2 Mise en place et mise à jour ..... 20
7.5.3 Maîtrise des informations documentées ..... 20

**8 Fonctionnement** ..... **21**
8.1 Planification et maîtrise opérationnelles ..... 21
8.2 Établissement des contrôles et des procédures ..... 21
8.3 Processus externalisés ..... 22

**9 Évaluation des performances** ..... **22**

© ISO 2014 – Tous droits réservés

9.1 Surveillance, mesure, analyse et évaluation ..... 22
9.1.1 Généralités ..... 22
9.1.2 Surveillance ..... 23
9.1.3 Sources de retour d'informations sur les performances de compliance ..... 23
9.1.4 Méthodes de collecte d'informations ..... 24
9.1.5 Analyse et classification des informations ..... 24
9.1.6 Mise en place des indicateurs ..... 25
9.1.7 Communication d'informations sur la compliance ..... 25
9.1.8 Contenu des rapports sur la compliance ..... 26
9.1.9 Conservation des enregistrements ..... 26
9.2 Audit ..... 27
9.3 Revue de direction ..... 27
**10 Amélioration ..... 28**
10.1 Non-conformité, non-compliance et actions correctives ..... 28
10.1.1 Généralités ..... 28
10.1.2 Remontée des informations ..... 29
10.2 Amélioration continue ..... 30
**Bibliographie ..... 31**

 © ISO 2014 – Tous droits réservés

# Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires.

Le comité chargé de l'élaboration du présent document est le Comité de Projet ISO/PC 271, *Systèmes de management de la conformité*.

© ISO 2014 – Tous droits réservés

# Introduction

Les organismes qui aspirent à garantir leur réussite sur le long terme doivent entretenir une culture d'intégrité et de compliance et prendre en compte les besoins et attentes des parties prenantes. L'intégrité et la compliance ne constituent donc pas seulement un prérequis mais également une opportunité pour un organisme florissant et durable.

La compliance est un résultat d'un organisme qui respecte ses obligations. La pérennité de la compliance est assurée par son intégration dans la culture de l'organisme ainsi que dans le comportement et la conduite des personnes qui travaillent en son sein. Tout en gardant son indépendance, il est préférable que le management de la compliance soit intégré aux processus de management de la finance, des risques, de la qualité, de l'environnement et de la santé et de la sécurité de l'organisme ainsi qu'à ses exigences et procédures opérationnelles.

Un système de management de la compliance efficace pour un organisme dans son ensemble permet à cette dernière de démontrer son engagement pour le respect de la législation en vigueur, ceci incluant les exigences légales, les codes industriels et les normes organisationnelles, ainsi que les standards de bonne gouvernance d'entreprise, les bonnes pratiques, l'éthique et les attentes des parties intéressées.

En ce qui concerne la compliance, l'approche d'un organisme est idéalement définie par un leadership qui applique ses valeurs fondamentales et les normes communément admises de gouvernance d'entreprise, d'éthique et communautaires. Intégrer la compliance dans le comportement des personnes qui travaillent pour un organisme dépend avant tout d'un leadership à tous les niveaux et de valeurs claires pour cet organisme, ainsi que de la reconnaissance et de la mise en œuvre de mesures pour promouvoir une attitude de compliance. Si cela n'est pas le cas à tous les niveaux d'un organisme, il y a risque de non-compliance.

Dans bon nombre de juridictions, pour déterminer la sanction appropriée à imposer en cas de non-respect des lois en vigueur, les tribunaux ont pris en compte l'engagement d'un organisme pour la compliance reflété par son système de management de la compliance. Par conséquent, les organismes de réglementation et judiciaire peuvent également bénéficier de la présente Norme internationale comme valeur de référence.

Les organismes sont de plus en plus convaincus du fait que l'application de valeurs engageantes et un management approprié de la compliance leur permettront de préserver leur intégrité et d'éviter ou de réduire les risques de non-respect de la loi. L'intégrité et une compliance efficaces sont donc des éléments clés pour un management avisé. La compliance contribue également au comportement socialement responsable des organismes.

La présente Norme internationale ne spécifie pas d'exigences, mais fournit des lignes directrices concernant les systèmes de management de la compliance et des pratiques recommandées. Les lignes directrices fournies dans la présente Norme internationale se veulent flexibles et l'utilisation de ces lignes directrices peut être différente selon la taille et le niveau de maturité du système de management de la compliance d'un organisme et selon le contexte, la nature et la complexité des activités de l'organisme, y compris sa politique et ses objectifs en matière de compliance.

L'organigramme de la Figure 1 est cohérent avec d'autres systèmes de management et est fondé sur le principe de l'amélioration continue (« Planifier-Mettre en œuvre-Contrôler-Agir »).


© ISO 2014 – Tous droits réservés

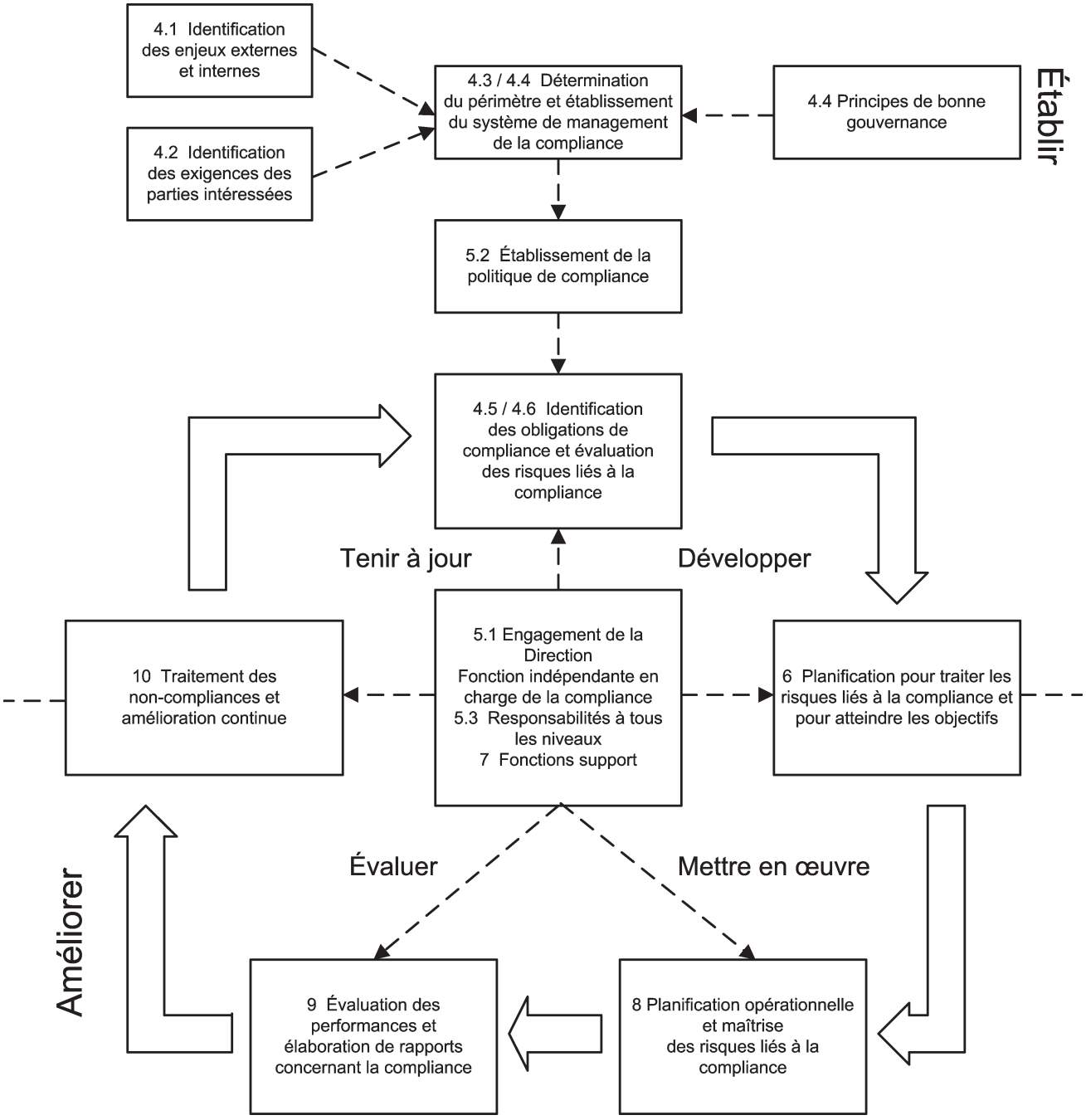



**Figure 1 — Schéma d'un système de management de la compliance**

La présente Norme internationale a adopté la « structure de niveau supérieur » (HLS) (c'est-à-dire, l'ordre des paragraphes, le texte de base identique et les termes et définitions de base communs) élaborées par l'ISO pour améliorer l'alignement entre ses diverses Normes internationales sur les systèmes de management. Outre ses recommandations générales sur le système de management de la compliance, la présente Norme internationale fournit également un cadre pour aider à la mise en œuvre dans tout système de management d'exigences spécifiques liées à la compliance.

Les organismes qui n'ont pas adopté de norme de systèmes de management, ou de cadre de management de la compliance, peuvent aisément adopter la présente Norme internationale comme lignes directrices autonomes au sein de leur organisme.

© ISO 2014 – Tous droits réservés

La présente Norme internationale est à même d'améliorer les exigences liées à la compliance dans d'autres systèmes de management et d'aider un organisme à améliorer le management dans son ensemble de toutes ses obligations de compliance.

La présente Norme internationale peut être combinée avec des normes de systèmes de management existantes (par exemple l'ISO 9001, l'ISO 14001, l'ISO 22000) et des lignes directrices génériques (par exemple l'ISO 31000, l'ISO 26000).


© ISO 2014 – Tous droits réservés

# Systèmes de management de la compliance — Lignes directrices

## 1 Domaine d'application

La présente Norme internationale fournit des lignes directrices relatives à l'établissement, au développement, à la mise en œuvre, à l'évaluation, à la maintenance et à l'amélioration d'un système de management de la compliance efficace et réactif au sein d'un organisme.

Les lignes directrices concernant les systèmes de management de la compliance sont applicables à tous les types d'organismes. L'étendue de l'application de ces lignes directrices dépend de la taille, de la structure, de la nature et de la complexité de l'organisme. La présente Norme internationale est basée sur les principes de bonne gouvernance, de proportionnalité, de transparence et de durabilité.

## 2 Références normatives

Il n'y a aucune référence normative.

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

**3.1**
**organisme**
personne ou groupe de personnes ayant sa propre structure fonctionnelle avec des responsabilités, autorités et relations en vue d'atteindre ses *objectifs* (3.9)

Note 1 à l'article: Le concept d'organisme comprend, sans toutefois s'y limiter, le travailleur indépendant, la compagnie, société, firme, entreprise, autorité, le partenariat, l'organisme caritatif ou institution, ou une partie ou une combinaison des entités précédentes, à responsabilité limitée ou d'un autre statut, de droit public ou privé.

**3.2**
**partie intéressée** (terme préféré)
**partie prenante** (terme admis)
personne ou *organisme* (3.1) qui peut avoir une incidence, être affectée ou se sentir affectée par une décision ou une activité

**3.3**
**direction**
personne ou groupe de personnes qui dirige et contrôle un *organisme* (3.1) au plus haut niveau

Note 1 à l'article: La direction a le pouvoir de déléguer son autorité et de fournir des ressources au sein de l'organisme.

Note 2 à l'article: Si le domaine d'application du *système de management* (3.7) traite uniquement une partie de l'organisme, alors la direction se réfère à ceux qui dirigent et contrôlent cette partie de l'organisme.

**3.4**
**organe directeur**
personne ou groupe de personnes qui administre un *organisme* (3.1), fixe les orientations et à qui la *direction* (3.3) rend compte

© ISO 2014 – Tous droits réservés