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 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

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*.

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 »).

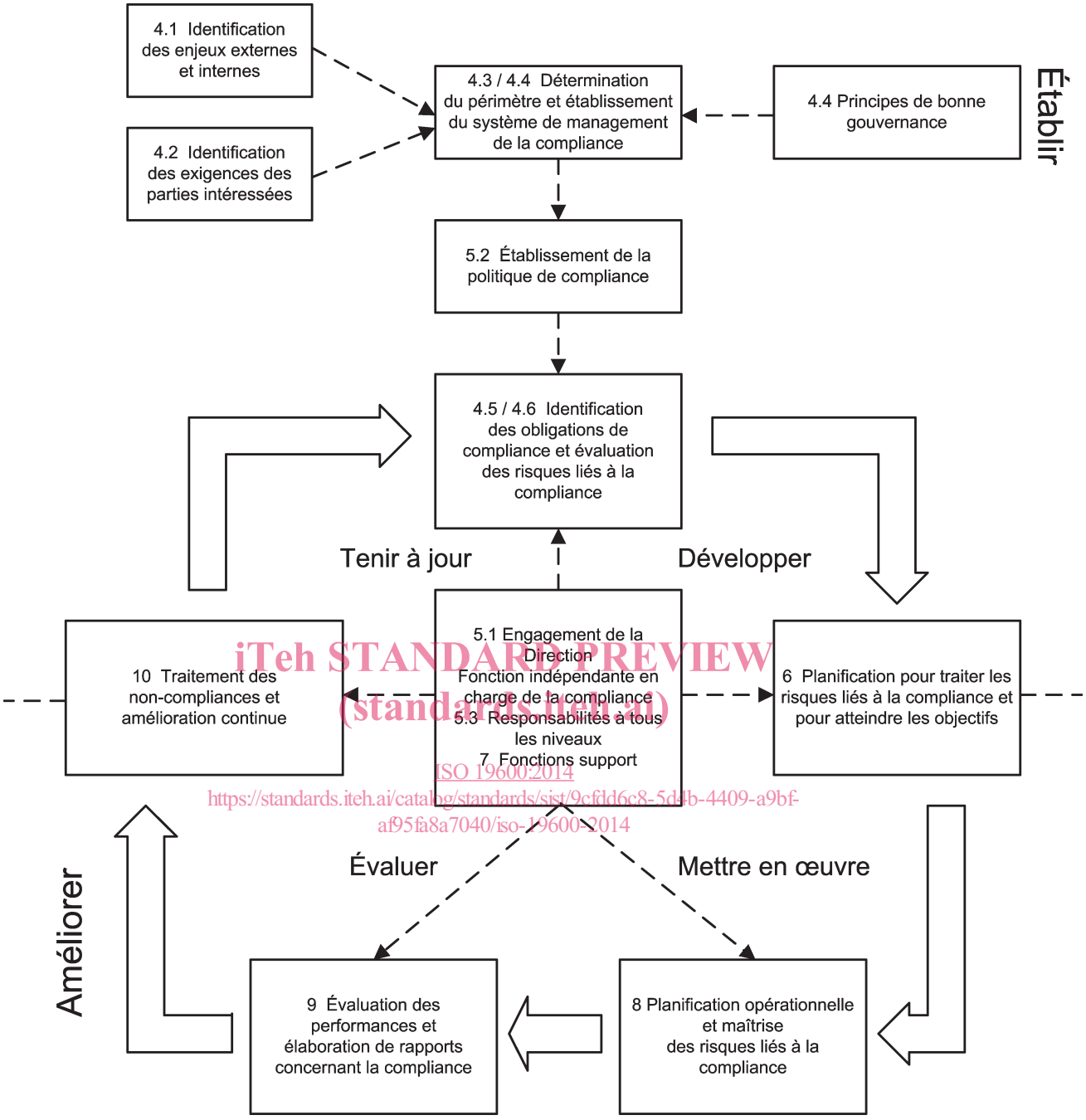

Figure 1 — Schéma d'un système de management de la compliance

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.

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).

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

3.5
employé
individu placé dans une relation reconnue comme étant une relation de travail, dans la législation nationale ou dans la pratique

3.6
fonction en charge de la compliance
personne(s) chargée(s) du management de la *compliance* (3.17)

Note 1 à l'article: Il est préférable que la responsabilité globale du management de la *compliance* (3.17) soit confiée à une seule personne.

3.7
système de management
ensemble d'éléments corrélés ou interactifs d'un *organisme* (3.1), utilisés pour établir des *politiques* (3.8) et des *objectifs* (3.9) et des *processus* (3.10) pour atteindre ces objectifs

Note 1 à l'article: Un système de management peut aborder une seule ou plusieurs disciplines.

Note 2 à l'article: Les éléments du système comprennent la structure organisationnelle, les rôles et responsabilités, la planification, le fonctionnement, etc.

Note 3 à l'article: Le domaine d'application d'un système de management peut comprendre l'ensemble de l'organisme, des fonctions spécifiques et identifiées de l'organisme, des sections spécifiques et identifiées de l'organisme, ou une ou plusieurs fonctions dans un groupe d'organismes.

3.8
politique
intentions et orientations d'un *organisme* (3.1), telles qu'elles sont officiellement formulées par sa *direction* (3.7)

3.9
objectif
résultat à atteindre

Note 1 à l'article: Un objectif peut être stratégique, tactique et/ou opérationnel.

Note 2 à l'article: Les objectifs peuvent être relatifs à différentes disciplines (telles que la finance, la santé et sécurité, et les buts environnementaux) et ils peuvent s'appliquer à divers niveaux (tels que stratégie, organisation dans son ensemble, projet, produit et *processus* (3.10)).

Note 3 à l'article: Un objectif peut être exprimé par d'autres façons, par exemple par un résultat escompté, un besoin, un critère opérationnel, en tant qu'objectif de compliance ou par l'utilisation d'autres termes ayant la même signification (par exemple fin, but ou cible).

Note 4 à l'article: Dans le contexte des normes de systèmes de management de la compliance, les objectifs de compliance sont établis par l'organisme, en cohérence avec sa politique en matière de compliance, en vue d'obtenir des résultats spécifiques.

3.10
processus
ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

3.11
risque
effet de l'incertitude sur l'atteinte des *objectifs* (3.9)

Note 1 à l'article: Un effet est un écart, positif ou négatif, par rapport à une attente.

Note 2 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Note 3 à l'article: Un risque est souvent caractérisé en référence à des « événements » potentiels ((tels que définis dans le ISO Guide 73:2009, 3.5.1.3) et des « conséquences » potentielles (telles que définies dans le le ISO Guide 73:2009, 3.6.1.3), ou une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa « vraisemblance » associée d'occurrence (telle que définie dans le ISO Guide 73:2009, 3.6.1.1).

3.12
risque lié à la compliance
effet de l'incertitude sur les *objectifs* (3.9) en matière de compliance

Note 1 à l'article: Le risque lié à la compliance peut être caractérisé par la vraisemblance d'occurrence et les conséquences de la *non-compliance* (3.18) aux *obligations de compliance* (3.16) de l'organisme.

3.13
exigence
besoin ou attente qui est formulé, généralement implicite ou obligatoire

Note 1 à l'article: « Généralement implicite » signifie qu'il est habituel ou de pratique commune pour l'organisme et les parties intéressées que le besoin ou l'attente à prendre en considération soit implicite.

Note 2 à l'article: Une exigence spécifiée est une exigence imposée, par exemple dans une information documentée.

3.14
exigence de compliance
exigence (3.13) à laquelle un *organisme* (3.1) doit se conformer

3.15
engagement de compliance
exigence (3.13) à laquelle un *organisme* (3.1) choisit de se conformer

3.16
obligation de compliance
exigence de compliance (3.14) ou *engagement de compliance* (3.15)

3.17
compliance
respect de toutes les *obligations de compliance* (3.16) d'un organisme

Note 1 à l'article: On pérennise la compliance en l'intégrant dans la culture d'un *organisme* (3.1) ainsi que dans le comportement et l'attitude des personnes travaillant au sein de cet organisme.

3.18
non-compliance
non-respect d'une *obligation de compliance* (3.16)

Note 1 à l'article: La non-compliance peut être un événement unique ou répété et il peut ou non être le résultat d'une *non-conformité* (3.33).

3.19
culture de la compliance
les valeurs, l'éthique et les convictions qui existent au sein d'un *organisme* (3.1) et interagissent avec les structures fonctionnelles et les systèmes de contrôle de l'organisme pour produire des normes comportementales conduisant aux résultats de *compliance* (3.17)

3.20
code
énoncé d'une pratique établie en interne ou par un organisme international, national ou sectoriel ou un autre *organisme* (3.1)

Note 1 à l'article: Le code peut être à caractère obligatoire ou à adhésion volontaire.

3.21
normes organisationnelles et sectorielles
ensemble documenté de *codes* (3.20), bonnes pratiques, chartes, normes techniques et sectorielles jugées pertinents par un *organisme* (3.1)

3.22
autorité réglementaire
organisme (3.1) chargée de régir ou de faire appliquer la *compliance* (3.17) aux *exigences* (3.17) légales et autres

3.23
compétence
capacité à mettre en pratique des connaissances et un savoir-faire pour obtenir les résultats escomptés

3.24
information documentée
information qui nécessite d'être contrôlée et tenue à jour par un *organisme* (3.1) et le format sur lequel elle est contenue

Note 1 à l'article: Les informations documentées peuvent se présenter dans tout format et sur tout support et provenir de toute source.

Note 2 à l'article: Les informations documentées peuvent se rapporter:

— au *système de management* (3.7), y compris les *processus* (3.10) associés;

— aux informations créées en vue du fonctionnement de l'organisme (documentation);

— aux preuves des résultats obtenus (enregistrements).

3.25
procédure
manière spécifiée de réaliser une activité ou un *processus* (3.10)

3.26
performance
résultat mesurable

Note 1 à l'article: La performance peut porter sur des constatations quantitatives ou qualitatives.

Note 2 à l'article: La performance peut concerner le management d'activités, de *processus* (3.10), de produits (y compris services), de systèmes ou d'*organismes* (3.1).

3.27
amélioration continue
activité ou *process*us (3.10) récurrents d'amélioration des *performance*s (3.26)

3.28
externaliser (verbe)
passer un accord en vertu duquel un *organisme* (3.1) externe assure une partie de la fonction ou met en œuvre une partie du *processus* (3.10) d'un organisme

Note 1 à l'article: L'organisme externe n'est pas inclus dans le périmètre du *système de management* (3.7), contrairement à la fonction ou au processus externalisé(e) qui en fait bien partie.

3.29
surveillance
détermination de l'état d'un système, d'un *process*us (3.10) ou d'une activité

Note 1 à l'article: Pour déterminer cet état, il peut être nécessaire de vérifier, superviser ou observer de façon critique.

Note 2 à l'article: La surveillance n'est pas une activité ponctuelle, mais un processus d'observation régulière ou continue d'une situation.

3.30
mesure
processus (3.10) visant à déterminer une valeur

3.31
audit
processus (3.10) méthodique, indépendant et documenté, permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

Note 1 à l'article: Un audit peut être interne (de première partie) ou externe (de seconde ou tierce partie), et il peut être combiné (s'il associe deux disciplines ou plus).

Note 2 à l'article: Les termes « preuves d'audit » et « critères d'audit » sont définis dans l'ISO 19011.

Note 3 à l'article: L'indépendance peut être démontrée par l'absence de responsabilité vis-à-vis de l'activité à auditer ou l'absence de divergence et de conflit d'intérêt.

3.32
conformité
satisfaction d'une **exigence** d'un système de management (3.13)

3.33
non-conformité
non-satisfaction d'une **exigence** d'un système de management (3.13)

Note 1 à l'article: Une non-conformité n'est pas nécessairement une *non-compliance* (3.18).

3.34
correction
action visant à éliminer une *non-conformité* (3.33) ou une *non-compliance* (3.18) détectée

3.35
action corrective
action visant à éliminer la cause d'une *non-conformité* (3.33) ou d'une *non-compliance* (3.18) et à éviter sa réapparition

4 Contexte de l'organisme

4.1 Connaissance de l'organisme et contexte

Il convient que l'organisme détermine les enjeux externes et internes, tels que ceux associés aux risques liés à la compliance, pertinents compte tenu de sa mission, et qui influent sur sa capacité à obtenir le(s) résultat(s) escompté(s) de son système de management de la compliance. Ce faisant, il convient que l'organisme prenne en compte une grande variété d'aspects externes et internes, tels que les contextes réglementaires, sociaux et culturels, la situation économique ainsi que les politiques, procédures, processus et ressources internes.

4.2 Compréhension des besoins et des attentes des parties intéressées

Il convient que l'organisme détermine:

— les parties intéressées qui sont concernées par le système de management de la compliance;

— les exigences de ces parties intéressées.