~~ISO/TC 309~~

~~Date :~~ 2021-04

ISO 37301:2021(F)

ISO/TC 309

Secrétariat~~:~~ BSI

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

Compliance management systems — Requirements with guidance for use

~~ICS : 03.100.01 ; 03.100.02 ; 03.100.70~~

~~Descripteurs :~~

Type du document : Norme internationale
Sous-type du document :
Stade du document : (60) Publication
Langue du document : F

Type du document : Norme internationale
Sous-type du document :
Stade du document : (60) Publication
Langue du document : F

Ch. de Blandonnet 8 • CPCase postale 401

• CH-1214 Vernier, Geneva, SwitzerlandGenève

Tel. Tél.: + 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~~www.iso.org/directives).

L'attention est attirée 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~~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 nature volontaire des normes, 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'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir ~~le lien suivant : www.iso.org/iso/fr/avant-propos~~www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 309, *Gouvernance des organisations*.

Cette première édition de l'ISO 37301 annule et remplace l'ISO 19600:2014, qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'ISO 19600:2014 sont les suivantes~~-~~:

— le présent document contient désormais des exigences et recommandations supplémentaires pour la mise en œuvre basées sur ces exigences~~-~~;

— le présent document suit les exigences de l'ISO pour une structure harmonisée des normes de systèmes de management.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse ~~www.iso.org/fr/members.html~~www.iso.org/fr/members.html.

Introduction

Les organismes qui aspirent à garantir leur réussite sur le long terme doivent établir et entretenir une culture de conformité, en prenant en compte les besoins et attentes des parties intéressées. Le dispositif de conformité ne constitue donc pas seulement un prérequis, mais également une opportunité pour un organisme qui souhaite se développer de façon durable.

La (mise/maintien en) conformité est un processus continu et le résultat d'un organisme qui exécute ses obligations. Le meilleur moyen de permettre l'instauration durable d'un dispositif de conformité est de l'intégrer à la culture de l'organisme ainsi que dans les attendus de l'organisme en matière de comportement et conduite du personnel. Tout en gardant son indépendance, il est préférable que la gestion du dispositif de conformité soit intégrée aux autres processus de l'organisme ainsi qu'à ses exigences et procédures opérationnelles.

L'existence d'un système de management de conformité, à l'échelle d'un organisme dans son ensemble, permet à ce dernier de démontrer son engagement vis-à-vis du respect de la législation en vigueur, y compris les exigences réglementaires, les codes industriels et les normes organisationnelles, ainsi que les normes de bonne gouvernance, les meilleures pratiques communément admises, l'éthique et les attentes des parties intéressées.

La démarche de (mise/maintien en) conformité d'un organisme est orientée par un leadership qui applique ses valeurs fondamentales et les principes communément admis de bonne gouvernance, d'éthique et communautaires. Intégrer la (mise/maintien en) conformité dans le comportement des personnes qui travaillent pour un organisme dépend avant tout d'une mission et d'une exemplarité 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 conformité. Si cela n'est pas le cas à tous les niveaux d'un organisme, un risque de défaut de conformité existe.

Dans plusieurs juridictions, pour déterminer la sanction appropriée à prononcer en cas de violation des lois en vigueur, les tribunaux ont tenu compte de l'engagement de l'organisme pour la (mise/maintien en) conformité soutenu par son système de management de conformité. Par conséquent, les autorités réglementaires/de régulation et les instances judiciaires peuvent également tirer parti du présent document comme référence.

Les organismes sont de plus en plus convaincus du fait qu'en appliquant des valeurs engageantes et une gestion appropriée de conformité, elles peuvent préserver leur intégrité et éviter ou de réduire le plus possible les cas de manquement aux obligations de conformité de l'organisme. L'intégrité et l'effectivité du dispositif de conformité sont donc des éléments clés pour une gestion saine et diligente de l'organisme. La (mise/maintien en) conformité contribue également au comportement socialement responsable des organismes.

L'un des objectifs du présent document est d'assister les organismes dans l'élaboration et la diffusion d'une culture positive de conformité, en considérant qu'il convient qu'une gestion efficace et saine des risques de conformité soit perçue comme étant une opportunité à saisir en raison des divers bénéfices qu'il procure à l'organisme, comme :

— l'amélioration des opportunités commerciales et de la viabilité économique/sociale/environnementale ;

— la protection et l'amélioration de la réputation et de la crédibilité d'un organisme ;

— la prise en compte des attentes des parties intéressées ;

— la démonstration de l'engagement d'un organisme vis-à-vis de la gestion effective de ses risques de conformité de manière efficace-;

— l'accroissement de la confiance des tierces parties dans la capacité de l'organisme à atteindre des objectifs sur le long terme-;

— la réduction au minimum de la violation ou de la menace de violation des lois, des coûts afférents et de l'atteinte à la réputation qui en découlent.

Le présent document spécifie des exigences relatives aux systèmes de management de conformité et fournit des recommandations et pratiques recommandées. Les exigences et les recommandations fournies dans le présent document se veulent flexibles et leur mise en œuvre peut être différente selon la taille et le niveau de maturité du système de management de conformité de l'organisme et selon le contexte, la nature et la complexité des activités de l'organisme et de ses objectifs.

Le présent document est à même d'améliorer les exigences de conformité dans d'autres systèmes de management et d'aider un organisme à améliorer la gestion dans son ensemble de toutes ses obligations de conformité.

La Figure 1 donne une vue d'ensemble des éléments les plus courants d'un système de management de conformité.

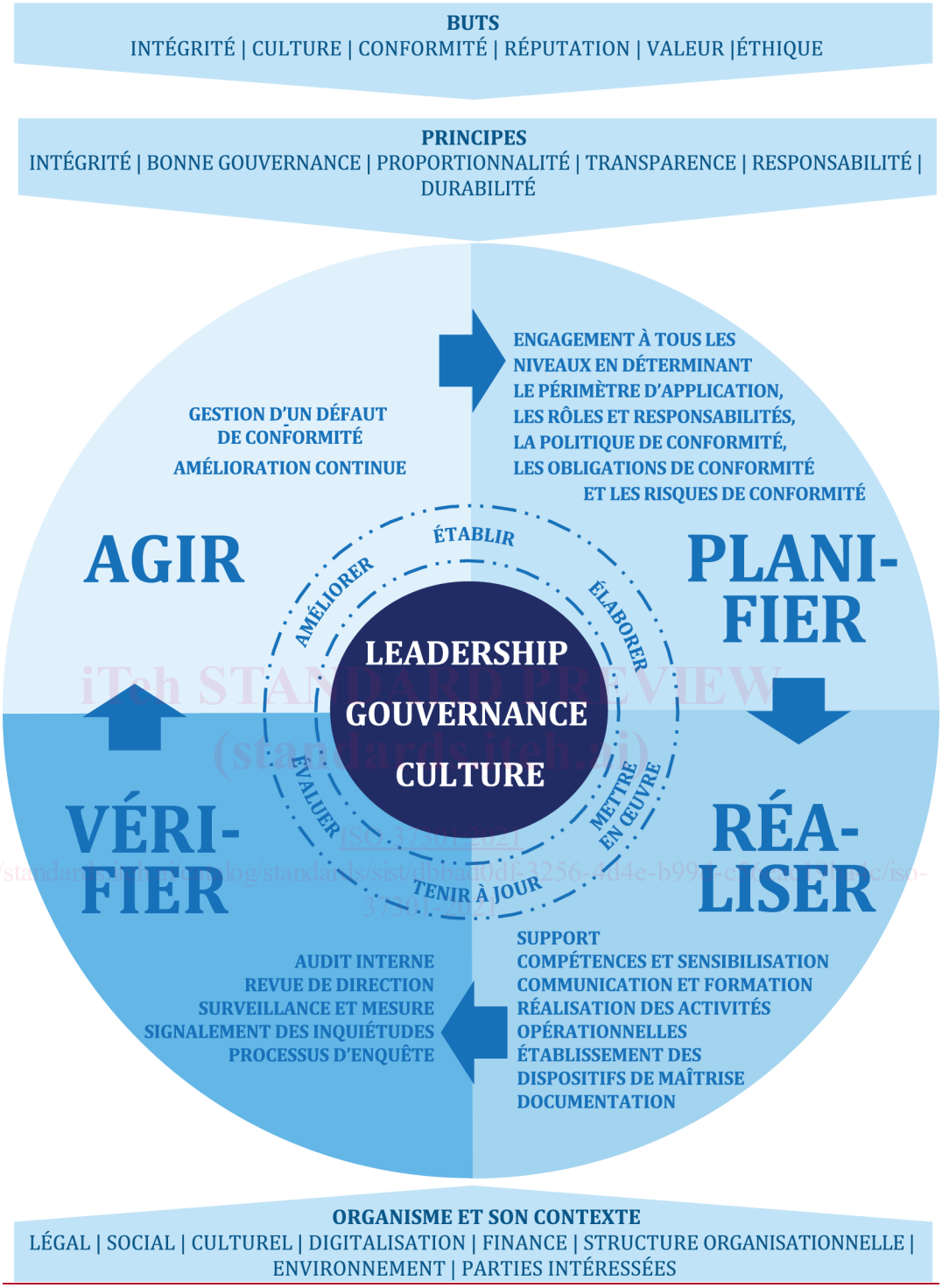

Figure 1 — Éléments d'un système de management de conformité

Dans le présent document, les formes verbales suivantes sont utilisées:

— «-doit-» indique une exigence-;

— «-il convient de/que-» indique une recommandation-;

— «-peut/il est admis-» («-» («may-» en anglais) indique une autorisation-;

— «-peut/il est possible-» (« ») («can-» en anglais) indique une possibilité ou une capacité.

Les informations sous forme de «-NOTE-» sont fournies pour clarifier l'exigence associée ou en faciliter la compréhension.

L'Annexe A donne des recommandations relatives à l'utilisation du présent document.

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

1 Domaine d'application

Le présent document spécifie des exigences et fournit des recommandations pour l'établissement, le développement, la mise en œuvre, l'évaluation, la tenue à jour et l'amélioration d'un système de management de conformité efficace au sein d'un organisme.

Le présent document s'applique à tous les types d'organismes, indépendamment du type, de la taille et de la nature de ses activités, qu'il appartienne au secteur public, privé ou à but non lucratif.

L'ensemble des exigences spécifiées dans le présent document qui font référence à un organe de gouvernance s'appliquent à la direction lorsque l'organe de gouvernance d'un organisme n'est pas distinct de la direction.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse ~~https://www.iso.org/obp~~ https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse ~~http://www.electropedia.org/~~ https://www.electropedia.org/

3.1
organisme
personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses *objectifs* (3.6)

Note 1 à l'article: Le concept d'organisme englobe sans s'y limiter, les travailleurs indépendants, les compagnies, les sociétés, les firmes, les entreprises, les administrations, les partenariats, les organisations caritatives ou les institutions, ou bien une partie ou une combinaison des entités précédentes, à responsabilité limitée ou ayant un autre statut, de droit public ou privé.

Note 2 à l'article: Si l'organisme fait partie d'une entité plus grande, le terme «organisme» se réfère uniquement à la partie de l'entité plus grande qui est couverte par le périmètre du système de management de conformité.

3.2
partie intéressée (terme préféré)
partie prenante (terme admis)
personne ou *organisme* (3.1) qui peut soit influer sur une décision ou une activité, soit être influencé(e) ou s'estimer influencé(e) par une décision ou une activité

3.3
direction
personne ou groupe de personnes qui oriente et dirige 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 périmètre du *système de management* (3.4) ne couvre qu'une partie de l'organisme, alors la direction s'adresse à ceux qui gouvernent et contrôlent cette partie de l'organisme.

Note 3 à l'article: Pour les besoins du présent document, le terme «-direction-» fait référence au plus haut niveau de direction exécutive.

3.4
système de management
ensemble d'éléments corrélés ou en interaction d'un *organisme* (3.1), utilisés pour établir des *politiques* (3.5) et des *objectifs* (3.6), ainsi que des *processus* (3.8) de façon à atteindre lesdits objectifs

Note 1 à l'article: Un système de management peut traiter d'un seul ou de plusieurs domaines.

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

3.5
politique
intentions et orientations d'un *organisme* (3.1), telles qu'elles sont officiellement formulées par sa *direction* (3.3)

Note 1 à l'article: Une politique peut également être officiellement formulée par l'*organe de gouvernance* (3.21) d'un organisme.

3.6
objectif
résultat à atteindre

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

Note 2 à l'article: Les objectifs peuvent se rapporter à différents domaines (tels que finance, ventes et marketing, achats, santé, sécurité, et environnement). Ils peuvent s'appliquer, par exemple, à l'organisme dans son ensemble ou à un projet, un produit, un service ou un *processus* (3.8).

Note 3 à l'article: Un objectif peut être exprimé de différentes manières, par exemple par un résultat escompté, un besoin, un critère opérationnel, en tant qu'objectif de *conformité* (3.26) ou par l'utilisation d'autres termes ayant la même signification (par exemple finalité, but ou cible).

Note 4 à l'article: Dans le contexte des *systèmes de management* (3.4) de conformité, les objectifs de conformité sont fixés par l'*organisme* (3.1), en cohérence avec sa *politique* (3.5) de conformité, en vue d'obtenir des résultats spécifiques.

3.7
risque

effet de l'incertitude sur l'atteinte des *objectifs* (3.6)

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 manque d'information qui entrave 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 par référence à des événements potentiels (tels que définis dans le Guide ISO 73) et à des conséquences également potentielles (telles que définies dans le Guide ISO 73), ou par référence à une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (y compris des changements de circonstances) et de la vraisemblance de son occurrence (telle que définie dans le Guide ISO 73).

3.8
processus
ensemble d'activités corrélées ou en interaction qui transforme des éléments d'entrée en résultat

Note 1 à l'article: Le résultat d'un processus est appelé «résultat», «», «produit» ou «service» en fonction du contexte de référence.

3.9
compétence
aptitude à mettre en pratique des connaissances et des savoir-faire pour obtenir les résultats escomptés

3.10
information documentée
information devant être maîtrisée et tenue à jour par un *organisme* (3.1) ainsi que le support sur lequel elle figure

Note 1 à l'article: Les informations documentées peuvent se présenter sous n'importe quel format et sur tous supports et peuvent provenir de toute source.

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

— au *système de management* (3.4), y compris les *processus* (3.8) connexes;

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

— aux preuves des résultats obtenus (enregistrements).

3.11
performance
résultat mesurable

Note 1 à l'article: Les performances peuvent être liées à des résultats quantitatifs ou qualitatifs.

Note 2 à l'article: Les performances peuvent concerner le management d'activités, de *processus* (3.8), de produits, de services, de systèmes ou d'*organismes* (3.1).

3.12
amélioration continue
activité récurrente menée pour améliorer les *performances* (3.11)

3.13
efficacité