

# PROJET DE NORME INTERNATIONALE

## ISO/DIS 37301

ISO/TC 309

Secrétariat: BSI

Début de vote:  
2020-03-13

Vote clos le:  
2020-06-05

---

---

## Systemes de management de la conformité — Exigences et recommandations pour la mise en oeuvre

*Compliance management systems — Requirements with guidance for use*

ICS: 03.100.01; 03.100.02; 03.100.70

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/FDIS 37301](https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301)

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301>

CE DOCUMENT EST UN PROJET DIFFUSÉ POUR OBSERVATIONS ET APPROBATION. IL EST DONC SUSCEPTIBLE DE MODIFICATION ET NE PEUT ÊTRE CITÉ COMME NORME INTERNATIONALE AVANT SA PUBLICATION EN TANT QUE TELLE.

OUTRE LE FAIT D'ÊTRE EXAMINÉS POUR ÉTABLIR S'ILS SONT ACCEPTABLES À DES FINS INDUSTRIELLES, TECHNOLOGIQUES ET COMMERCIALES, AINSI QUE DU POINT DE VUE DES UTILISATEURS, LES PROJETS DE NORMES INTERNATIONALES DOIVENT PARFOIS ÊTRE CONSIDÉRÉS DU POINT DE VUE DE LEUR POSSIBILITÉ DE DEVENIR DES NORMES POUVANT SERVIR DE RÉFÉRENCE DANS LA RÉGLEMENTATION NATIONALE.

LES DESTINATAIRES DU PRÉSENT PROJET SONT INVITÉS À PRÉSENTER, AVEC LEURS OBSERVATIONS, NOTIFICATION DES DROITS DE PROPRIÉTÉ DONT ILS AURAIENT ÉVENTUELLEMENT CONNAISSANCE ET À FOURNIR UNE DOCUMENTATION EXPLICATIVE.

Le présent document est distribué tel qu'il est parvenu du secrétariat du comité.



Numéro de référence  
ISO/DIS 37301:2020(F)

© ISO 2020

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/FDIS 37301](https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301)

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301>



**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO 2020

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en oeuvre, 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, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée 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 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Tél.: +41 22 749 01 11  
Fax: +41 22 749 09 47  
E-mail: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Publié en Suisse

## Sommaire

Page

Avant-propos.....	v
Introduction .....	vi
<b>1</b> <b>Domaine d'application .....</b>	<b>1</b>
<b>2</b> <b>Références normatives.....</b>	<b>1</b>
<b>3</b> <b>Termes et définitions.....</b>	<b>1</b>
<b>4</b> <b>Contexte de l'organisme.....</b>	<b>6</b>
4.1 <b>Connaissance de l'organisme et contexte .....</b>	<b>6</b>
4.2 <b>Compréhension des besoins et des attentes des parties intéressées .....</b>	<b>6</b>
4.3 <b>Détermination du périmètre d'application du système de management de la conformité.....</b>	<b>7</b>
4.4 <b>Système de management de la conformité.....</b>	<b>7</b>
<b>5</b> <b>Leadership.....</b>	<b>7</b>
5.1 <b>Leadership et engagement .....</b>	<b>7</b>
5.1.1 <b>Organe de gouvernance et direction .....</b>	<b>7</b>
5.1.2 <b>Culture de la conformité .....</b>	<b>8</b>
5.1.3 <b>Gouvernance relative à la conformité .....</b>	<b>8</b>
5.2 <b>Politique.....</b>	<b>9</b>
5.3 <b>Rôles, responsabilités et autorités .....</b>	<b>9</b>
5.3.1 <b>Organe de gouvernance et direction .....</b>	<b>9</b>
5.3.2 <b>Fonction en charge de la conformité.....</b>	<b>10</b>
5.3.3 <b>Encadrement .....</b>	<b>11</b>
5.3.4 <b>Personnel.....</b>	<b>12</b>
<b>6</b> <b>Planification.....</b>	<b>12</b>
6.1 <b>Actions à mettre en œuvre face aux risques et opportunités .....</b>	<b>12</b>
6.2 <b>Objectifs de conformité et planification des actions pour les atteindre .....</b>	<b>13</b>
6.3 <b>Obligations de conformité .....</b>	<b>13</b>
6.4 <b>Évaluation des risques liés à la conformité.....</b>	<b>13</b>
<b>7</b> <b>Support.....</b>	<b>14</b>
7.1 <b>Ressources .....</b>	<b>14</b>
7.2 <b>Compétences.....</b>	<b>14</b>
7.2.1 <b>Généralités .....</b>	<b>14</b>
7.2.2 <b>Processus relatif à l'emploi .....</b>	<b>14</b>
7.2.3 <b>Formation .....</b>	<b>15</b>
7.3 <b>Sensibilisation.....</b>	<b>15</b>
7.4 <b>Communication.....</b>	<b>15</b>
7.5 <b>Informations documentées.....</b>	<b>16</b>
7.5.1 <b>Généralités .....</b>	<b>16</b>
7.5.2 <b>Création et mise à jour des informations documentées.....</b>	<b>17</b>
7.5.3 <b>Maîtrise des informations documentées .....</b>	<b>17</b>
<b>8</b> <b>Réalisation des activités opérationnelles.....</b>	<b>17</b>
8.1 <b>Planification et maîtrise opérationnelles .....</b>	<b>17</b>
8.2 <b>Établissement des contrôles et des procédures .....</b>	<b>18</b>
8.3 <b>Signalement des inquiétudes .....</b>	<b>18</b>
8.4 <b>Processus d'enquête.....</b>	<b>18</b>
<b>9</b> <b>Évaluation des performances.....</b>	<b>19</b>
9.1 <b>Surveillance, mesure, analyse et évaluation.....</b>	<b>19</b>

9.1.1	Généralités .....	19
9.1.2	Sources de retour d'informations sur les performances de conformité .....	19
9.1.3	Mise en place des indicateurs.....	19
9.1.4	Communication d'informations sur la conformité .....	19
9.1.5	Conservation des enregistrements.....	20
9.2	Audit interne .....	20
9.3	Revue de direction .....	21
10	Amélioration.....	22
10.1	Non-conformité aux exigences, état de non-conformité et actions correctives.....	22
10.2	Amélioration continue.....	22
Annexe A (informative) Recommandations relatives à l'utilisation du présent document.....		23
Bibliographie.....		47

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/FDIS 37301](https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301)

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301>

## 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](http://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](http://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](http://www.iso.org/iso/fr/avant-propos).

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

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](http://www.iso.org/fr/members.html).

Le présent document annule et remplace l'ISO 19600:2014-10.

Dans la présente Norme internationale, 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.

## Introduction

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

La conformité est un processus continu et le résultat d'un organisme qui respecte ses obligations. La pérennité de la conformité est assurée par son intégration à 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 conformité soit intégré aux autres processus de management de l'organisme ainsi qu'à ses exigences et procédures opérationnelles.

Un système de management de la conformité efficace, 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 légales, les codes industriels et les normes organisationnelles, ainsi que les standards de bonne gouvernance d'entreprise, les meilleures pratiques, l'éthique et les attentes des parties intéressées.

L'approche de la conformité d'un organisme est orientée par une direction qui applique ses valeurs fondamentales et les normes communément admises de gouvernance d'entreprise, d'éthique et communautaires. Intégrer la conformité dans le comportement des personnes qui travaillent pour un organisme dépend avant tout d'une direction 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 non-conformité existe.

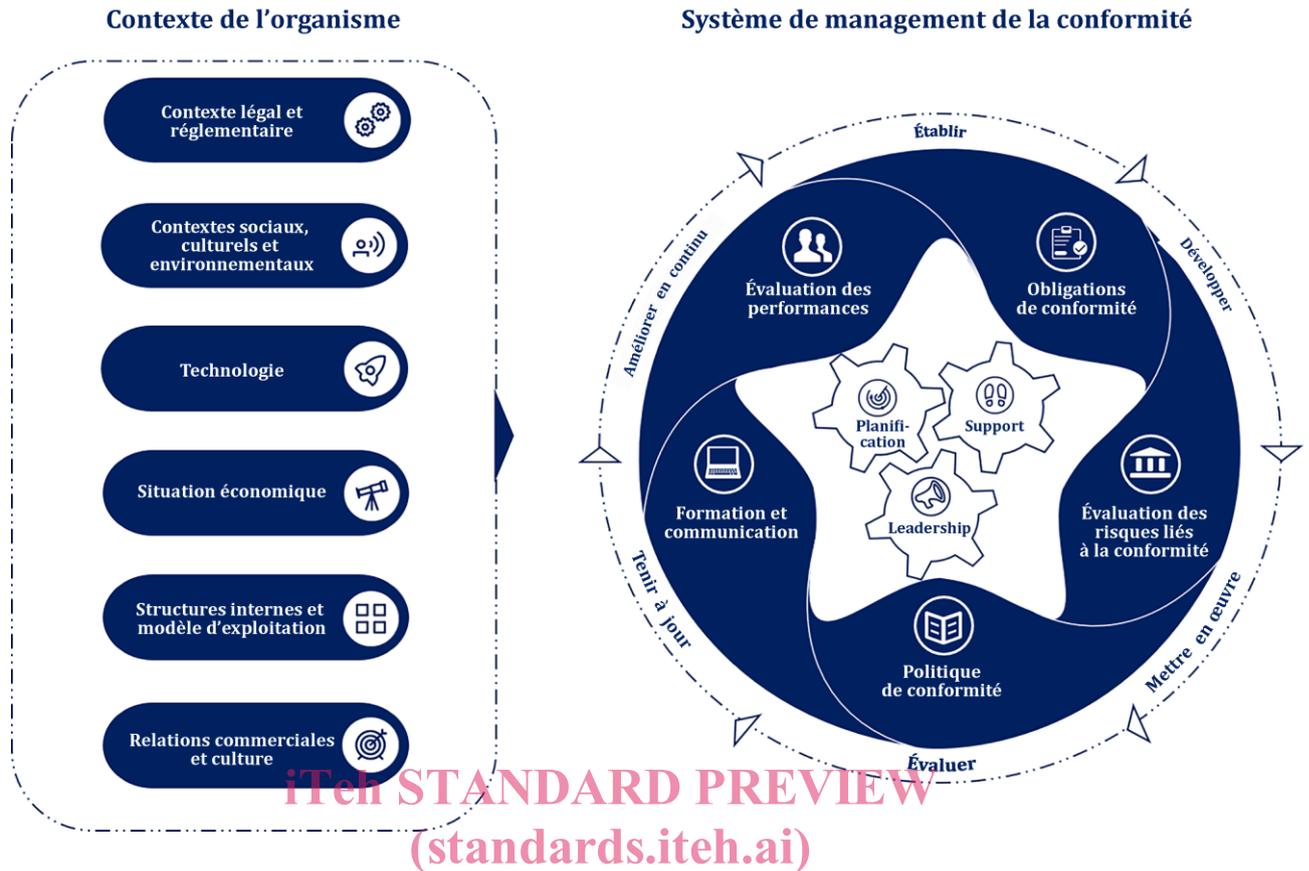
Dans plusieurs juridictions, pour déterminer la sanction appropriée à imposer en cas de non-respect des lois en vigueur, les tribunaux ont pris en compte l'engagement de l'organisme pour la conformité soutenu par son système de management de la conformité. Par conséquent, les régulateurs et les instances judiciaires peuvent également tirer parti du présent document comme référence.

Les organismes sont de plus en plus convaincus du fait que l'application de valeurs engageantes et un management approprié de la conformité leur permettront de préserver leur intégrité et d'éviter ou de réduire les risques de non-respect des obligations de conformité de l'organisme. L'intégrité et l'effectivité de la conformité sont donc des éléments clés pour un management avisé. La 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 la conformité, en considérant qu'il convient qu'un management efficace et sain des risques liés à la conformité soit perçu comme étant une opportunité à saisir en raison des divers bienfaits qu'il procure à l'organisme.

Le présent document spécifie des exigences et fournit des recommandations relatives aux systèmes de management de la conformité et aux 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 la conformité d'un 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 liées à la conformité dans d'autres systèmes de management et d'aider un organisme à améliorer le management dans son ensemble de toutes ses obligations de conformité.



**ITeH STANDARD PREVIEW**  
**(standards.iteh.ai)**

**Figure 1**

[ISO/FDIS 37301](https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301)

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301>

# 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 un cadre directeur pour l'établissement, le développement, la mise en œuvre, l'évaluation, la tenue à jour et l'amélioration d'un système de management de la 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 (standards.iteh.ai)

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> ;
- IEC Electropedia : disponible à l'adresse <http://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* (3.8)

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.

### 3.2

#### partie intéressée (terme préféré)

partie prenante (terme admis)

personne ou *organisme* (3.1) qui peut soit influencer sur une décision ou une activité, soit être influencé(e) ou s'estimer influencé(e) par une décision ou une activité

### 3.3

#### **exigence**

besoin ou attente qui sont formulés, généralement implicites ou obligatoires

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 formulée, par exemple une information documentée.

### 3.4

#### **système de management**

ensemble d'éléments corrélés ou en interaction d'un *organisme* (3.1), utilisés pour établir des *politiques* (3.7) et des *objectifs* (3.8), et des *processus* (3.12) 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 comprennent la structure, les rôles et responsabilités, la planification et le fonctionnement de l'organisme.

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

### 3.5

#### **direction**

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

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

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

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c58cae7ba4c/iso-37301>

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.

### 3.6

#### **efficacité**

niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

### 3.7

#### **politique**

intentions et orientations d'un *organisme* (3.1), telles qu'elles sont officiellement formulées par sa *direction* (3.5) et/ou son *organe de gouvernance* (3.22)

### 3.8

#### **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, santé, sécurité, et environnement) et peuvent s'appliquer à divers niveaux [au niveau stratégique, à un niveau concernant l'organisme dans son ensemble ou afférant à un projet, un produit ou un *processus* (3.12), par exemple].

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 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 de la conformité, les objectifs de conformité sont fixés par l'organisme, en cohérence avec sa politique de conformité, en vue d'obtenir des résultats spécifiques.

### 3.9

#### risque

effet de l'incertitude

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).

### 3.10

#### compétence

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

### 3.11

#### 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 (3.12) connexes ;
- aux informations créées en vue du fonctionnement de l'organisme (documentation) ;
- aux preuves des résultats obtenus (enregistrements).

### 3.12

#### processus

ensemble d'activités corrélées ou en interaction qui transforme des éléments d'entrée en éléments de sortie

### 3.13

#### 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 (3.12), de produits (y compris de services), de systèmes ou d'organismes (3.1).

### 3.14

#### **externaliser**

passer un accord selon lequel un *organisme* (3.1) externe assure une partie de la fonction ou met en œuvre une partie du *processus* (3.11) d'un organisme

Note 1 à l'article : L'organisme externe n'est pas inclus dans le périmètre du *système de management* (3.4), contrairement à la fonction ou au processus externalisé qui en font partie intégrante.

### 3.15

#### **surveillance**

détermination de l'état d'un système, d'un *processus* (3.12) ou d'une activité

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

### 3.16

#### **mesure**

*processus* (3.12) visant à déterminer une valeur

### 3.17

#### **audit**

*processus* (3.12) 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 domaines ou plus).

Note 2 à l'article : Un audit interne est réalisé par l'organisme lui-même ou par une partie externe pour le compte de celui-ci.

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-57e2c19b461d/iso-dis-37301>

Note 3 à l'article : Les termes « preuves d'audit » et « critères d'audit » sont définis dans l'ISO 19011.

Note 4 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'intérêts.

### 3.18

#### **conformité (à une exigence)**

satisfaction d'une *exigence* (3.3)

### 3.19

#### **non-conformité (à une exigence)**

non-satisfaction d'une *exigence* (3.3)

Note 1 à l'article : Une non-conformité n'est pas nécessairement un *état de non-conformité* (3.28).

### 3.20

#### **action corrective**

action visant à éliminer la ou les causes d'une *non-conformité* (3.19) ou d'un *état de non-conformité* (3.28) et à éviter qu'elle ne réapparaisse

### 3.21

#### **amélioration continue**

activité récurrente menée pour améliorer les *performances* (3.13)

**3.22****organe de gouvernance**

personne ou groupe de personnes qui détient la responsabilité et l'autorité ultimes des activités, de la gouvernance et des politiques d'un *organisme* (3.1), à qui la *direction* (3.5) rend compte de ses décisions et par laquelle/lequel celle-ci est tenue responsable

Note 1 à l'article : Tous les organismes, particulièrement les petits organismes, ne disposeront pas d'un organe de gouvernance distinct de la direction.

Note 2 à l'article : Un organe de gouvernance peut notamment comprendre le conseil d'administration, les comités du conseil, le conseil de surveillance, les administrateurs ou les superviseurs.

**3.23****personnel**

individus placés dans une relation reconnue comme étant une relation de travail dans la législation nationale ou dans la pratique, ou dans toute relation contractuelle dont l'existence dépend de l'*organisme* (3.1)

**3.24****fonction en charge de la conformité**

personne ou groupe de personnes qui détient la responsabilité et l'autorité vis-à-vis du fonctionnement du *système de management* (3.4) de la *conformité* (3.27)

Note 1 à l'article : De préférence, la supervision du système de management de la conformité sera attribuée à un seul individu.

(standards.iteh.ai)

**3.25****risque lié à la conformité**

vraisemblance d'occurrence et les conséquences de la *non-conformité* (3.17) aux *obligations de conformité* (3.26) de l'*organisme*

**3.26****obligation de conformité**

*exigences* (3.3) auxquelles un *organisme* (3.1) doit obligatoirement se conformer, ainsi que celles auxquelles un *organisme* (3.1) choisit volontairement de se conformer

**3.27****conformité****état de conformité**

résultat du respect de toutes les *obligations de conformité* (3.26) d'un organisme

**3.28****non-conformité****état de non-conformité**

non-respect d'une *obligation de conformité* (3.26)

**3.29****culture de la conformité**

valeurs, éthique et 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 à l'*état de conformité* (3.27)

### 3.30

#### **conduite**

comportements et pratiques d'un organisme qui influent sur les résultats pour les clients, employés, fournisseurs, marchés et communautés

### 3.32

#### **tierce partie**

personne ou organe indépendant(e) de l'*organisme* (3.1)

Note 1 à l'article : Tous les associés métiers sont des tierces parties, mais toutes les tierces parties ne sont pas des associés métiers.

### 3.33

#### **procédure**

manière spécifiée de réaliser une activité ou un *processus* (3.12)

[SOURCE : ISO 9000:2015, 3.4.5]

## 4 Contexte de l'organisme

### 4.1 Connaissance de l'organisme et contexte

L'organisme doit déterminer les enjeux externes et internes pertinents par rapport à sa finalité, et qui influent sur sa capacité à atteindre le ou les résultats attendus de son système de management de la conformité.

(standards.iteh.ai)

À cette fin, l'organisme doit prendre en compte un vaste éventail d'enjeux, notamment :

- contexte légal et réglementaire ;
- contextes sociaux, culturels et environnementaux ;
- technologies ;
- situation économique ;
- structures, politiques, procédures, processus et ressources internes ;
- modèle d'exploitation, y compris la stratégie, la nature, la taille, la portée ainsi que la complexité et la pérennité des activités et opérations de l'organisme ;
- nature et étendue des relations métiers avec des tierces parties ;
- culture de la conformité actuelle.

### 4.2 Compréhension des besoins et des attentes des parties intéressées

L'organisme doit déterminer :

- les parties intéressées qui sont pertinentes dans le cadre du système de management de la conformité ;
- les exigences de ces parties intéressées.

### 4.3 Détermination du périmètre d'application du système de management de la conformité

L'organisme doit déterminer les limites et l'applicabilité du système de management de conformité afin d'établir son périmètre d'application.

NOTE Le périmètre du système de management de la conformité vise à clarifier les principaux risques de conformité auxquels l'organisme est confronté ainsi que les limites géographiques et/ou organisationnelles dans lesquelles le système de management de la conformité s'appliquera, en particulier si l'organisme fait partie d'un organisme plus grand.

Lorsque l'organisme établit ce périmètre, il doit prendre en compte :

- les enjeux externes et internes auxquels il est fait référence en 4.1 ;
- les exigences auxquelles il est fait référence en 4.2 et 6.3.

Le périmètre d'application doit être disponible sous la forme d'une information documentée.

### 4.4 Système de management de la conformité

L'organisme doit établir, mettre en œuvre, évaluer, tenir à jour et améliorer en continu un système de management de la conformité, y compris les processus nécessaires et leurs interactions, en accord avec les exigences du présent document.

Le système de management de la conformité doit refléter les valeurs, les objectifs, la stratégie et les risques de conformité de l'organisme, en tenant compte du contexte de l'organisme (voir 4.1).

<https://standards.iteh.ai/catalog/standards/sist/dbbad0df-3256-4d4e-b99d-c56eac19ba4c/iso-fdis-37301>

## 5 Leadership

### 5.1 Leadership et engagement

#### 5.1.1 Organe de gouvernance et direction

L'organe de gouvernance et la direction doivent démontrer leur leadership et engagement vis-à-vis du système de management de la conformité en :

- s'assurant que la politique et les objectifs sont établis pour le système de management de la conformité et qu'ils sont compatibles avec l'orientation stratégique de l'organisme ;
- s'assurant que les exigences liées au système de management de la conformité sont intégrées aux processus métiers de l'organisme ;
- s'assurant que les ressources requises pour le système de management de la conformité sont disponibles ;
- communiquant sur l'importance de disposer d'un système de management de la conformité efficace et de se conformer aux exigences liées à ce système ;
- veillant à ce que le système de management de la conformité atteigne le ou les résultats attendus ;
- orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du système de management de la conformité ;

- promouvant l'amélioration continue ;
- soutenant les autres rôles managériaux pertinents afin de démontrer leur implication dans leurs domaines respectifs.

NOTE Dans le présent document, il convient d'interpréter le terme « métier » au sens large, c'est-à-dire comme se référant aux activités liées à la finalité de l'organisme.

L'organe de gouvernance et la direction doivent :

- établir et faire respecter les valeurs fondamentales de l'organisme ;
- s'assurer que des politiques, procédures et processus sont élaborés et mis en œuvre afin d'atteindre les objectifs de conformité ;
- s'assurer qu'ils sont informés de manière opportune sur les sujets liés à la conformité, y compris sur les instances de non-conformité, et veiller à ce que des actions appropriées soient prises ;
- s'assurer que l'engagement à l'égard de la conformité est maintenu et que la non-conformité et les comportements non respectueux des règles de conformité sont traités de manière appropriée ;
- s'assurer que les responsabilités en matière de conformité sont incluses dans les descriptions de postes le cas échéant ;
- désigner une fonction en charge de la conformité (voir 5.3.2).

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

### 5.1.2 Culture de la conformité

L'organisme doit développer, entretenir et promouvoir une culture de la conformité à tous les niveaux de l'organisme.

L'organe de gouvernance, la direction et le personnel d'encadrement doivent démontrer un engagement actif, visible, cohérent et durable envers le comportement qui est exigé de tous dans l'ensemble de l'organisme.

La direction doit encourager les comportements qui engendrent et soutiennent la conformité, et doit empêcher et ne pas tolérer les comportements qui la compromettent.

### 5.1.3 Gouvernance relative à la conformité

L'organe de gouvernance et la direction doivent s'assurer que les principes suivants sont mis en œuvre :

- accès direct de la fonction en charge de la conformité à l'organe de gouvernance ;
- indépendance de la fonction en charge de la conformité ;
- autorité et compétence appropriées de la fonction en charge de la conformité.

NOTE 1 L'accès direct peut inclure : ligne hiérarchique directe avec l'organe de gouvernance, soumission de rapports périodiques à l'organe de gouvernance et participation à ses réunions.

NOTE 2 Indépendance signifie absence de toute interférence et/ou pression illégitime avec la fonction en charge de la conformité.