

---

---

## Systèmes de management des alertes — Lignes directrices

*Whistleblowing management systems — Guidelines*

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

[ISO 37002:2021](https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021)

<https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021>



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

ISO 37002:2021

<https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021>



### DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2021

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, 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, Genève

Tél.: +41 22 749 01 11

E-mail: [copyright@iso.org](mailto:copyright@iso.org)

Web: [www.iso.org](http://www.iso.org)

Publié en Suisse

## Sommaire

Page

<b>Avant-propos</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Domaine d'application</b> .....	<b>1</b>
<b>2 Références normatives</b> .....	<b>1</b>
<b>3 Termes et définitions</b> .....	<b>1</b>
<b>4 Contexte de l'organisme</b> .....	<b>7</b>
4.1 Compréhension de l'organisme et de son contexte.....	7
4.2 Compréhension des besoins et attentes des parties intéressées.....	8
4.3 Détermination du périmètre d'application du système de management des alertes.....	8
4.4 Système de management des alertes.....	9
<b>5 Leadership</b> .....	<b>10</b>
5.1 Leadership et engagement.....	10
5.1.1 Organe de gouvernance.....	10
5.1.2 Direction.....	10
5.2 Politique d'alerte.....	11
5.3 Rôles, responsabilités et autorités au sein de l'organisme.....	12
5.3.1 Direction et organe de gouvernance.....	12
5.3.2 Fonction de management des alertes.....	12
5.3.3 Délégation de la prise de décision.....	13
<b>6 Planification</b> .....	<b>13</b>
6.1 Actions à mettre en œuvre face aux risques et opportunités.....	13
6.2 Objectifs du système de management des alertes et planification des actions pour les atteindre.....	14
6.3 Planification des changements.....	15
<b>7 Soutien</b> .....	<b>15</b>
7.1 Ressources.....	15
7.2 Compétences.....	15
7.3 Sensibilisation.....	16
7.3.1 Généralités.....	16
7.3.2 Formation et mesures de sensibilisation du personnel.....	16
7.3.3 Formation pour les dirigeants et autres rôles spécifiques.....	17
7.4 Communication.....	18
7.5 Informations documentées.....	19
7.5.1 Généralités.....	19
7.5.2 Création et mise à jour des informations documentées.....	19
7.5.3 Maîtrise des informations documentées.....	19
7.5.4 Protection des données.....	20
7.5.5 Confidentialité.....	20
<b>8 Réalisation des activités opérationnelles</b> .....	<b>21</b>
8.1 Planification et maîtrise opérationnelles.....	21
8.2 Réception des signalements d'actes répréhensibles.....	24
8.3 Évaluation des signalements d'actes répréhensibles.....	25
8.3.1 Évaluation de l'acte répréhensible signalé.....	25
8.3.2 Évaluation et prévention des risques de mesures de représailles.....	26
8.4 Traitement des signalements d'actes répréhensibles.....	27
8.4.1 Traitement de l'acte répréhensible signalé.....	27
8.4.2 Protection et soutien du lanceur d'alerte.....	28
8.4.3 Traitement des mesures de représailles.....	28
8.4.4 Protection de la ou des personnes faisant l'objet d'un signalement.....	29
8.4.5 Protection des parties intéressées concernées.....	29
8.5 Clôture des cas d'alertes.....	29

<b>9</b>	<b>Évaluation des performances</b> .....	<b>30</b>
9.1	Surveillance, mesure, analyse et évaluation.....	30
9.1.1	Généralités.....	30
9.1.2	Indicateurs d'évaluation.....	31
9.1.3	Sources d'information.....	31
9.2	Audit interne.....	32
9.2.1	Généralités.....	32
9.2.2	Programme d'audit interne.....	32
9.3	Revue de direction.....	33
9.3.1	Généralités.....	33
9.3.2	Entrées de la revue de direction.....	33
9.3.3	Résultats de la revue de direction.....	33
<b>10</b>	<b>Amélioration</b> .....	<b>33</b>
10.1	Amélioration continue.....	33
10.2	Non-conformité et actions correctives.....	34
	<b>Bibliographie</b> .....	<b>35</b>

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

[ISO 37002:2021](https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021)

<https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021>

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

## Introduction

L'alerte est l'acte qui consiste à signaler un acte répréhensible présumé ou un risque d'acte répréhensible. Les études et l'expérience montrent qu'une grande partie des actes répréhensibles est portée à l'attention de l'organisme concerné par le biais de signalements émanant de personnes au sein ou proches de l'organisme.

Les organismes envisagent de plus en plus de mettre en place ou d'améliorer des politiques et des processus d'alerte internes en réponse à la réglementation ou sur la base du volontariat.

Le présent document fournit des recommandations aux organismes pour établir, mettre en œuvre, tenir à jour et améliorer un système de management des alertes, avec les résultats suivants:

- a) encourager et faciliter le signalement des actes répréhensibles;
- b) soutenir et protéger les lanceurs d'alerte et les autres parties intéressées impliquées;
- c) veiller à ce que les signalements d'actes répréhensibles soient traités de manière appropriée et dans les meilleurs délais;
- d) améliorer la culture de l'organisme et la gouvernance;
- e) réduire les risques d'actes répréhensibles.

Les avantages potentiels pour l'organisme sont notamment les suivants:

- permettre à l'organisme d'identifier et de traiter les actes répréhensibles le plus tôt possible;
- aider à prévenir ou à réduire le plus possible la perte d'actifs et faciliter la récupération des actifs perdus;
- assurer le respect des politiques et procédures de l'organisme, ainsi que des obligations légales et sociales;
- attirer et retenir le personnel attaché aux valeurs et à la culture de l'organisme;
- faire la démonstration de pratiques de gouvernance saines et éthiques à la société, aux marchés, aux organismes de réglementation et de contrôle aux propriétaires et aux autres parties intéressées.

Un système efficace de management des alertes permet d'instaurer la confiance au sein de l'organisme en:

- démontrant l'engagement des dirigeants à prévenir et à traiter les actes répréhensibles;
- encourageant tout un chacun à se manifester sans tarder pour signaler les actes répréhensibles;
- réduisant et prévenant les préjudices subis par les lanceurs d'alerte et les autres personnes impliquées;
- favorisant une culture d'ouverture, de transparence, d'intégrité et de redevabilité.

Le présent document fournit des recommandations aux organismes pour créer un système de management des alertes, fondé sur les principes de confiance, d'impartialité et de protection. Il est adaptable, et son utilisation variera en fonction de la taille, de la nature, de la complexité et de la juridiction des activités de l'organisme. Il peut aider un organisme à améliorer sa politique et ses procédures d'alerte existantes, ou à se conformer à la législation applicable aux lanceurs d'alerte.

Le présent document adopte la «structure harmonisée» (c'est-à-dire succession des articles, texte commun et terminologie commune) élaborée par l'ISO afin d'améliorer l'alignement entre les Normes internationales de systèmes de management. Les organismes peuvent adopter le présent document comme guide autonome pour leur organisation ou en même temps que d'autres normes de systèmes de

management, notamment pour répondre aux exigences relatives aux alertes dans d'autres systèmes de management ISO.

La [Figure 1](#) est une représentation conceptuelle d'un système recommandé de management des alertes, montrant comment les principes de confiance, d'impartialité et de protection couvrent tous les éléments d'un tel système.

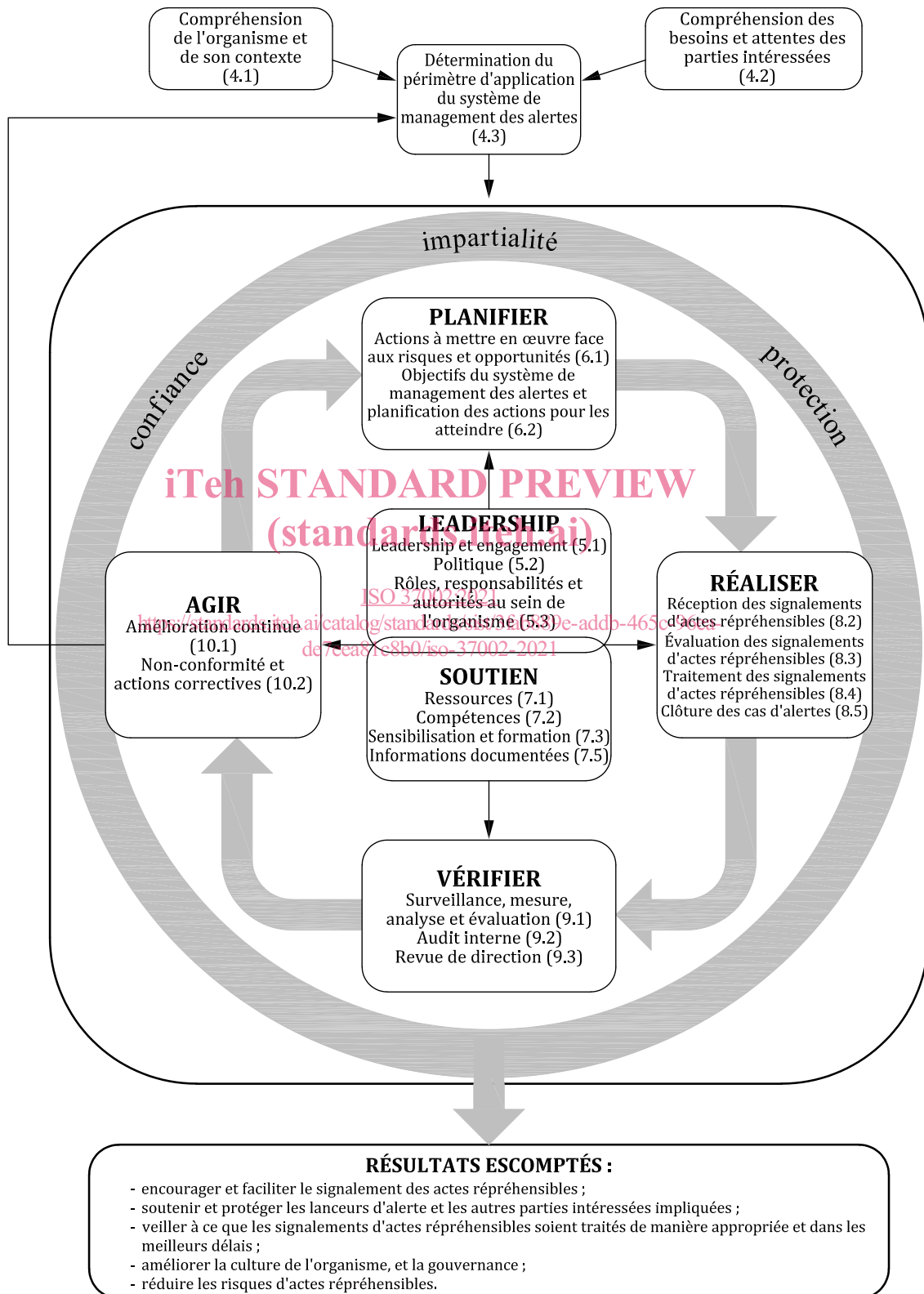


Figure 1 — Vue d'ensemble d'un système de management des alertes

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

ISO 37002:2021

<https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021>



# Systèmes de management des alertes — Lignes directrices

## 1 Domaine d'application

Le présent document fournit des lignes directrices pour établir, mettre en œuvre et tenir à jour un système de management des alertes efficace, fondé sur les principes de confiance, d'impartialité et de protection et comprenant les quatre étapes suivantes:

- a) réception des signalements d'actes répréhensibles;
- b) évaluation des signalements d'actes répréhensibles;
- c) traitement des signalements d'actes répréhensibles;
- d) clôture des cas d'alertes.

Les lignes directrices du présent document sont génériques et destinées à s'appliquer à tous les organismes, indépendamment du type, de la taille et de la nature de l'activité, qu'ils évoluent dans le secteur public, privé ou à but non lucratif.

L'étendue de l'application de ces lignes directrices dépend des facteurs décrits en 4.1, 4.2 et 4.3. Le système de management des alertes peut être autonome ou peut être utilisé dans le cadre d'un système de management global.

## 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>
- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>

### 3.1

#### systeme de management

ensemble d'éléments corrélés ou en interaction d'un *organisme* (3.2), utilisés pour établir des *politiques* (3.7) et des *objectifs* (3.25), ainsi que des *processus* (3.27) 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.

Note 3 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

## 3.2

### **organisme**

personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses *objectifs* (3.25)

Note 1 à l'article: Le concept d'organisme englobe, sans toutefois 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» fait uniquement référence à la partie de cette entité faisant partie intégrante du périmètre du *système de management* (3.1) *des alertes* (3.10).

Note 3 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

## 3.3

### **personnel**

directeurs, agents, employés, contractuels ou personnel intérimaire et bénévoles de l'*organisme* (3.2)

[SOURCE: ISO 37001:2016, 3.25, modifiée — Les Notes 1 et 2 à l'article ont été supprimées.]

## 3.4

**partie intéressée** (terme recommandé)

**partie prenante (terme admis)**

personne ou *organisme* (3.2) 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

Note 1 à l'article: Une partie intéressée peut être interne ou externe à l'organisme.

Note 2 à l'article: Les parties intéressées peuvent inclure, sans toutefois s'y limiter, les auteurs de signalements, les personnes faisant l'objet de signalements, les témoins, le *personnel* (3.3), les représentants des travailleurs, les fournisseurs, les tiers, le public, les médias, les organismes de réglementation et de contrôle et l'organisme dans son ensemble.

Note 3 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO. La définition originale a été modifiée par l'ajout des Notes 1 et 2 à l'article.

## 3.5

### **direction**

personne ou groupe de personnes qui oriente et dirige un *organisme* (3.2) 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* (3.1) ne couvre qu'une partie de l'organisme, alors la direction s'adresse à ceux qui orientent et dirigent cette partie de l'organisme.

Note 3 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

## 3.6

### **organe de gouvernance**

personne ou groupe de personnes qui détient la *responsabilité* (3.30) ultime de l'ensemble de l'*organisme* (3.2)

Note 1 à l'article: Chaque entité organisationnelle dispose d'un organe de gouvernance, qu'il soit ou non explicitement établi.

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

[SOURCE: ISO/IEC 38500:2015, 2.9, modifiée — Les mots «détient la responsabilité ultime» remplacent «est responsable du fonctionnement et de la conformité de» et les Notes 1 et 2 à l'article ont été ajoutées.]

### 3.7

#### politique

intentions et orientations d'un *organisme* (3.2) telles qu'elles sont officiellement formulées par sa *direction* (3.5)

Note 1 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.8

#### acte répréhensible

action(s) ou omission(s) pouvant causer un préjudice

Note 1 à l'article: Les actes répréhensibles peuvent comprendre, sans toutefois s'y limiter, les pratiques suivantes:

- violation de la loi (nationale ou internationale), comme la fraude, la corruption, y compris les pots-de-vin;
- violation du code de conduite de l'*organisme* (3.2) ou d'un autre code de conduite pertinent, violation des *politiques* de l'*organisme* (3.7);
- négligence grave, intimidation, harcèlement, discrimination, utilisation non autorisée de fonds ou de ressources, abus d'autorité, conflit d'intérêts, gaspillage flagrant ou mauvaise gestion;
- les actions ou omissions entraînant un dommage ou un risque de préjudice pour les droits de l'homme, l'environnement, la santé et la sécurité publiques, des pratiques de travail sûres ou l'intérêt public.

Note 2 à l'article: Un acte répréhensible ou le préjudice qui en résulte peut s'être produit dans le passé, être en train de se produire ou peut se produire à l'avenir.

Note 3 à l'article: Le préjudice potentiel peut être déterminé par référence à un événement unique ou à une série d'événements.

<https://standards.iteh.ai/catalog/standards/sist/3fab889e-addb-465c-96ea-de7eea81c8b0/iso-37002-2021>

### 3.9

#### lanceur d'alerte

personne qui signale des *actes répréhensibles* (3.8) présumés ou réels et a des motifs raisonnables de croire que les informations sont exactes au moment du signalement

Note 1 à l'article: Un motif raisonnable est une conviction d'un individu s'appuyant sur l'observation, l'expérience ou des informations en sa possession qu'une personne dans les mêmes circonstances partagerait également.

Note 2 à l'article: Les exemples de lanceurs d'alerte incluent ce qui suit, sans toutefois s'y limiter:

- le *personnel* (3.3) d'un *organisme* (3.2);
- le personnel de parties externes, y compris les personnes morales, avec lesquelles l'organisme a, ou prévoit d'établir, une certaine forme de relation d'affaires, y compris, sans toutefois s'y limiter, les clients, les entreprises communes (ou joint-ventures), les partenaires d'entreprise commune, les partenaires de consortium, les prestataires de services externalisés, les sous-traitants, les consultants, les sous-contractants, les fournisseurs, les revendeurs, les conseillers, les agents, les distributeurs, les représentants, les intermédiaires et les investisseurs;
- d'autres personnes comme les représentants syndicaux;
- toute personne ayant occupé ou devant occuper une fonction mentionnée dans cette définition.

### 3.10

#### alerte

signalement d'*actes répréhensibles* (3.8) présumés ou réels par un *lanceur d'alerte* (3.9)

Note 1 à l'article: Un signalement d'actes répréhensibles peut être verbal, en personne, par écrit ou sous forme électronique ou numérique.

Note 2 à l'article: Il est courant de faire une distinction entre:

- une alerte transparente où le lanceur d’alerte divulgue des informations sans dissimuler son identité ou exiger que son identité soit gardée secrète;
- une alerte confidentielle où l’identité et toute information pouvant permettre d’identifier le lanceur d’alerte sont connues du destinataire mais ne sont pas divulguées sans le consentement du lanceur d’alerte, sauf si la loi l’exige;
- une alerte anonyme où l’information est reçue sans que le lanceur d’alerte ne révèle son identité.

Note 3 à l'article: Les *organismes* (3.2) peuvent utiliser un autre terme tel que «procédure d’alerte», «alerte interne», «alerte professionnelle» ou «whistleblowing» ou un équivalent.

### 3.11

#### fonction de management des alertes

personne(s) qui détien(nen)t la responsabilité et l’autorité du fonctionnement du *système de management* (3.1) *des alertes* (3.10)

### 3.12

#### triage

évaluation du signalement initial *d’actes répréhensibles* (3.8) à des fins de catégorisation, de prise de mesures préliminaires, de priorisation et d’affectation pour traitement ultérieur

Note 1 à l'article: Les facteurs suivants peuvent être pris en compte: la probabilité et la gravité de l’impact des actes répréhensibles sur le *personnel* (3.3), l’*organisme* (3.2) et les *parties intéressées* (3.4), y compris les dommages à la réputation, financiers, environnementaux, humains ou autres.

### 3.13

#### mesure de représailles

iTeh STANDARD PREVIEW

menace, intention, action ou omission, directe ou indirecte, susceptible de porter préjudice à un *lanceur d’alerte* (3.9) ou à une autre *partie intéressée* (3.4), en lien avec l’*alerte* (3.10)

Note 1 à l'article: Le préjudice comprend toute conséquence négative, qu’elle soit professionnelle ou personnelle, y compris, sans toutefois s’y limiter, le licenciement, la suspension, la rétrogradation, le transfert, le changement de fonctions, la modification des conditions de travail, les mauvaises notes de *performance* (3.26), des mesures disciplinaires, la réduction des possibilités d’avancement, le refus de services, l’inscription sur une liste noire, le boycottage, l’atteinte à la réputation, la divulgation de l’identité du lanceur d’alerte, la perte financière, les poursuites ou les actions en justice, le harcèlement, l’isolement ou toute forme de préjudice physique ou psychologique.

Note 2 à l'article: Les mesures de représailles comprennent les représailles, les sanctions, les actions ou omissions délibérées, faites sciemment ou par négligence pour porter préjudice à un lanceur d’alerte ou à d’autres parties concernées.

Note 3 à l'article: Les mesures de représailles comprennent également l’incapacité à prévenir ou à réduire le plus possible le préjudice en assurant un degré de diligence raisonnable à chaque étape du *processus* d’alerte (3.27).

Note 4 à l'article: Les actions visant à traiter les propres *actes répréhensibles* (3.8), les performances ou la gestion d’un lanceur d’alerte, indépendamment de son rôle dans le signalement, ne constituent pas une mesure de représailles au regard du présent document.

Note 5 à l'article: Les autres parties intéressées concernées peuvent inclure les lanceurs d’alerte potentiels ou présumés, les proches, les associés d’un lanceur d’alerte, des personnes qui ont apporté leur soutien à un lanceur d’alerte, et toute personne impliquée dans un processus d’alerte, y compris les personnes morales.

### 3.14

#### enquête

*processus* (3.27) méthodique, indépendant et documenté, permettant d’établir des faits et de les évaluer de manière objective pour déterminer si des *actes répréhensibles* (3.8) ont eu lieu, ont lieu ou risquent d’avoir lieu et dans quelle mesure

Note 1 à l'article: Une enquête peut être interne ou externe. Il peut s’agir d’une enquête combinée.

Note 2 à l'article: Une enquête interne est menée par l’*organisme* (3.2) lui-même ou par une partie externe pour le compte de celui-ci.

Note 3 à l'article: Une enquête peut également être imposée à l'organisme par des parties externes.

### 3.15 audit

*processus* (3.27) méthodique et indépendant, permettant d'obtenir des preuves 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 (3.2) lui-même ou par une partie externe pour le compte de celui-ci.

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: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.16 compétence

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

Note 1 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.17 conformité

satisfaction d'une *exigence* (3.28)

Note 1 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.18 non-conformité

non-satisfaction d'une *exigence* (3.28)

Note 1 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.19 action corrective

action visant à éliminer la cause d'une *non-conformité* (3.18) et à éviter qu'elle ne réapparaisse

Note 1 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.20 amélioration continue

activité récurrente menée pour améliorer les *performances* (3.26)

Note 1 à l'article: Ceci constitue l'un des termes communs et l'une des principales définitions de la structure harmonisée des normes de systèmes de management ISO.

### 3.21 information documentée

information devant être maîtrisée et tenue à jour par un *organisme* (3.2) 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* (3.1), y compris les *processus* (3.27) connexes;