Norme internationale

ISO 37003

Systèmes de management anti-fraude — Recommandations pour les organismes gérant le risque de fraude

Fraud control management systems — Guidance for organizations managing the risk of fraud

Première édition
2025-05

Numéro de référence
ISO 37003:2025(fr)

DOCUMENT PROTÉGÉ PAR DROIT D'AUTEUR

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

Web: www.iso.org

Publié en Suisse

Licence et conditions d'utilisation

Comme indiqué ci-dessus, les documents ISO, ainsi que toute mise à jour et/ou correction, et tout droit de propriété intellectuelle ou autre droit y afférent, sont la propriété de l'ISO. Les documents ISO sont distribués sous licence, et non vendus. Le présent document ne saurait en aucun cas avoir pour effet de céder ou de transférer quelque droit de propriété intellectuelle que ce soit de l'ISO à l'utilisateur. Les documents ISO sont protégés par le droit d'auteur, la législation relative aux bases de données, le droit des marques, la législation en matière de concurrence déloyale, la législation relative au secret commercial et toute autre disposition légale applicable. Les utilisateurs reconnaissent et acceptent de respecter les droits de propriété intellectuelle de l'ISO sur les documents ISO.

L'utilisation des documents ISO est soumise aux conditions de l'accord de licence applicable.

Les documents ISO sont fournis dans le cadre de différents types d'accords de licence («Type de licence») offrant un droit non exclusif, non transférable, limité et révocable d'utilisation des documents ISO ou d'accès à ces derniers aux fins décrites ci-dessous («Finalité»), dont le champ d'application peut être interne ou externe. La ou les finalités visées doivent être fixées dans le bon de commande et/ou dans l'accord de licence applicable.

a) Type de licence:

   1) Licence pour utilisateur final enregistré unique (document filigrané au nom de l'utilisateur) aux fins spécifiées. Sous cette licence, l'utilisateur n'est pas autorisé à partager le document ISO concerné avec qui que ce soit, y compris sur un réseau.

2) Licence pour mise en réseau aux fins spécifiées. La licence pour mise en réseau peut être octroyée soit à des utilisateurs finaux simultanés non désignés, soit à des utilisateurs finaux simultanés désignés au sein d'une même organisation.

b) Finalité:

1) Finalité interne. Usage interne uniquement au sein de l'organisation de l'utilisateur, y compris, mais sans s'y limiter, aux fins de sa propre mise en œuvre («Finalité interne»).

Les possibilités d'usage interne autorisé sont spécifiées au moment de l'achat ou dans le cadre d'un accord ultérieur avec l'ISO, l'organisme membre de l'ISO dans le pays de l'utilisateur, tout autre organisme membre de l'ISO ou un distributeur tiers autorisé, y compris tout droit d'utilisation à des fins internes applicable (par exemple, réunions internes, programmes de formation en interne, préparation de services de certification, illustration de manuels internes, supports de formation en interne et documents d'orientation internes, ou intégration dans ces derniers). Chaque usage interne doit être explicitement spécifié dans le bon de commande et/ou dans l'accord de licence applicable, et des frais et exigences spécifiques s'appliquent à chaque usage autorisé.

2) Finalité externe. Usage externe, y compris, mais sans s'y limiter:

— les services d'essai;

— les services d'inspection;

— les services de certification;

— les services d'audit;

— les services de conseil;

— l'élaboration et la mise en œuvre de programmes d'évaluation de la conformité;

— les services de formation;

— l'enseignement;

— la recherche;

— le développement de logiciels et autres plateformes numériques ou services numériques reposant sur des logiciels;

— toute autre activité ou tout autre service proposé par l'utilisateur ou l'organisation de l'utilisateur à une tierce partie, à des fins commerciales ou non commerciales («Finalité externe»).

Les possibilités d'usage externe autorisé sont spécifiées au moment de l'achat ou dans le cadre d'un accord ultérieur avec l'ISO, l'organisme membre de l'ISO dans le pays de l'utilisateur, tout autre organisme membre de l'ISO ou un distributeur tiers autorisé, y compris tout droit d'utilisation à des fins externes applicable (par exemple, dans des publications, des produits ou des services commercialisés et vendus par l'utilisateur/l'organisation de l'utilisateur). Chaque usage externe doit être explicitement spécifié dans le bon de commande et/ou dans l'accord de licence applicable, et des frais et exigences spécifiques s'appliquent à chaque usage autorisé.

Hormis les cas où les utilisateurs ont obtenu des droits d'utilisation conformément aux dispositions susmentionnées, ils ne sont pas autorisés à partager les documents ISO ou à octroyer des sous-licences au sein ou à l'extérieur de leur organisation, quelle que soit la finalité. Les utilisateurs qui souhaiteraient obtenir des droits d'utilisation additionnels pour des documents ISO ou leur contenu sont invités à prendre contact avec l'ISO ou le membre de l'ISO dans leur pays pour étudier les différentes options envisageables.

Lorsque l'utilisateur ou l'organisation de l'utilisateur se voit octroyer une licence à des fins externes de fourniture de l'un des services suivants à une tierce partie:

— services d'essai;

— services d'inspection;

— services de certification;

— services d'audit;

— services de conseil;

et dans le cas où l'un des cinq (5) services susmentionnés fait référence à, s'appuie sur, incorpore ou utilise de quelque manière que ce soit un point, une exigence, une disposition ou toute autre information figurant dans un document ISO, l'utilisateur ou l'organisation de l'utilisateur s'engage à vérifier que la tierce partie bénéficiant desdits services a elle-même obtenu auprès de l'organisme membre de l'ISO dans son pays, de tout autre organisme membre de l'ISO, de l'ISO ou d'un distributeur tiers autorisé, une licence valide pour la mise en œuvre du document ISO correspondant ou pour tout autre usage en rapport avec les services susmentionnés. Cette obligation de vérification est prévue aux termes de l'accord de licence applicable obtenu par l'utilisateur ou l'organisation de l'utilisateur.

Les documents ISO ne doivent pas être divulgués à des tiers, et les utilisateurs doivent les utiliser uniquement aux fins spécifiées dans le bon de commande et/ou l'accord de licence applicable. La divulgation ou l'utilisation non autorisée des documents ISO à des fins autres que celles pour lesquelles une licence a été octroyée est interdite et peut entraîner des poursuites judiciaires.

Restrictions d'utilisation

Sauf disposition contraire dans l'accord de licence applicable et sous réserve de l'octroi d'une licence distincte par l'ISO, l'organisme membre de l'ISO dans le pays de l'utilisateur, tout autre organisme membre de l'ISO ou un distributeur tiers autorisé, les utilisateurs ne sont pas autorisés à:

— utiliser des documents ISO à toute autre fin que la Finalité prévue;

— octroyer des droits d'utilisation des documents ISO ou des droits d'accès à ceux-ci hors du cadre du Type de licence concerné;

— divulguer des documents ISO hors du cadre de la Finalité et/ou du Type de licence prévus;

— vendre, prêter, louer, reproduire, distribuer, importer/exporter ou exploiter commercialement de quelque manière que ce soit des documents ISO. Dans le cas des documents publiés conjointement (par exemple les documents ISO/IEC), cette clause s'applique à la cotitularité des droits d'auteur respectifs;

— céder ou transférer de quelque manière que ce soit la propriété des documents ISO, en tout ou en partie, à un tiers.

Indépendamment du type de licence ou de la finalité pour laquelle les utilisateurs se voient octroyer des droits d'accès et d'utilisation pour des documents ISO, les utilisateurs ne sont pas autorisés à accéder aux documents ISO ou à les utiliser, en tout ou en partie, à des fins d'apprentissage automatique et/ou pour une intelligence artificielle et/ou à des fins similaires, y compris, mais sans s'y limiter

a) en tant que données d'entraînement de grands modèles de langage ou de modèles similaires, ou

b) pour des invites ou pour permettre à une intelligence artificielle ou à des outils similaires de générer des réponses.

Un tel usage n'est autorisé que s'il fait l'objet d'un accord de licence spécifique conclu avec l'organisme membre de l'ISO dans le pays du demandeur, un autre organisme membre de l'ISO ou l'ISO. Les demandes d'autorisation de cette nature sont examinées au cas par cas afin de garantir le respect des droits de propriété intellectuelle. En particulier, l'exception au droit d'auteur visée à l'Article 4 de la Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique ne saurait être invoquée aux fins de la fouille de textes et de données sur les documents ISO, l'ISO renonçant par la présente à cette exception.

En cas de doute raisonnable de l'ISO ou de l'organisme membre de l'ISO dans le pays de l'utilisateur quant au respect des présentes conditions par l'utilisateur, l'ISO ou l'organisme membre de l'ISO concerné peut exiger par écrit de réaliser un audit, ou de faire réaliser un audit par un auditeur tiers, pendant les heures ouvrables, dans les locaux de l'utilisateur ou via un accès à distance.

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'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse http://www.iso.org/patents. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

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.

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 http://www.iso.org/members.html.

Introduction

La fraude constitue un risque pour tous les organismes, qu'ils relèvent des secteurs privé, public ou à but non lucratif. Les cas de fraude peuvent avoir des répercussions significatives sur la situation financière de l'organisme cible et entraînent souvent des conséquences financières indirectes sur les économies locales et mondiales. La fraude peut entraîner de graves conséquences juridiques et financières, ainsi que des dommages psychologiques et émotionnels durables pour les personnes concernées. Pour un aperçu des types de fraude couramment rencontrés par les organismes, voir l'Annexe A.

La généralisation et la sophistication croissantes des technologies de l'information, l'adoption rapide des systèmes de paiement électroniques par la population dans son ensemble et la mondialisation de l'économie ont entraîné une augmentation des attaques frauduleuses externes contre les organismes dans tous les secteurs.

Il convient que les leaders (organe de gouvernance, équipe de direction, rôles pertinents) de tous les organismes prennent en considération la gestion et la maîtrise du risque de fraude.

NOTE Pour plus d'informations sur la fraude en lien avec la gouvernance, voir l'ISO 37000:2021, 6.9.

Le présent document fournit des recommandations relatives:

a) à la création et la tenue à jour de processus pour repérer, apprécier le risque de fraude et en assurer la surveillance;

b) à l'atténuation des fraudes internes et externes, y compris celles commises à l'encontre de l'organisme ou par celui-ci;

c) à la détection des fraudes commises à l'encontre de l'organisme ou par celui-ci, sur la base de ses expositions présumées au risque de fraude;

d) à une remédiation efficace aux cas de fraude afin de s'assurer que:

   — les atteintes à l'image de l'organisme peuvent être réduites le plus possible;

   — sa réputation peut être rétablie et renforcée;

   — les fonds perdus à la suite d'une fraude peuvent être récupérés;

e) à l'inscription dans une dynamique d'amélioration continue.

L'application de ces recommandations ne peut assurer qu'aucune fraude n'a eu ou n'aura lieu à l'avenir, car il n'est pas possible d'éliminer le risque de fraude. Cependant, elles aident les organismes à gérer efficacement le risque de fraude, à répondre de manière appropriée aux cas de fraude et à éviter ou à réduire le risque de responsabilité en matière de conformité.

Une maîtrise/un contrôle efficace de la fraude exige que l'organisme s'engage dans des dispositifs de prévention, de détection et de remédiation, fondées sur le leadership, la planification et l'allocation de ressources, comme cela est résumé à la Figure 1.

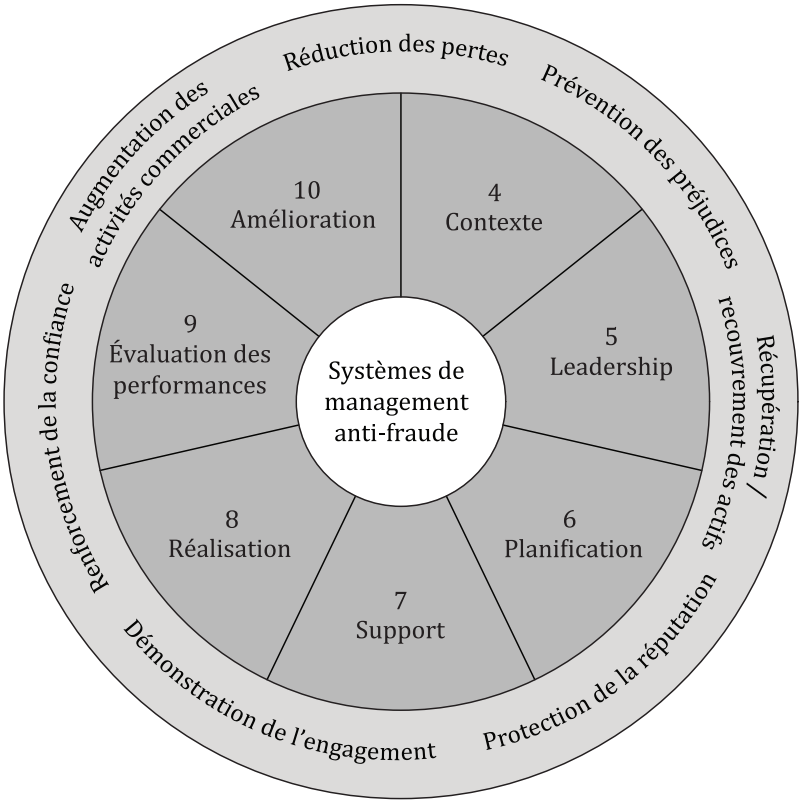

Figure 1 — Principes, structure et objectifs du présent document

Systèmes de management anti-fraude — Recommandations pour les organismes gérant le risque de fraude

1 Domaine d'application

Le présent document fournit des recommandations pour les organismes pour le développement, la mise en œuvre et le maintien d'un système de management anti-fraude (FCMS, de l'anglais *Fraud Control Management System*) efficace. Celui-ci inclut la prévention de la fraude, la détection précoce des actes frauduleux et une remédiation efficace aux cas de fraude survenus ou susceptibles de survenir.

Il fournit également des recommandations pour la gestion du risque de fraude, comprenant:

a) la fraude interne commise à l'encontre de l'organisme;

b) la fraude externe commise à l'encontre de l'organisme;

c) la fraude interne commise en collaboration avec des partenaires commerciaux ou d'autres tiers;

d) la fraude externe commise en collaboration avec le personnel de l'organisme;

e) la fraude commise par l'organisme lui-même ou par des personnes prétendant agir en son nom et dans son intérêt.

Le présent document s'applique à tous les organismes, quels que soient leur type, leur taille, la nature de leurs activités, que ces organismes relèvent du secteur public ou privé, à but lucratif ou non lucratif. Il n'est pas destiné à aider les consommateurs à prévenir, à détecter ou à lutter contre ce qui est généralement appelé la «fraude à la consommation».

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 https://www.electropedia.org/

3.1
fraude
acte malhonnête intentionnel entraînant un gain ou une perte, réel(le) ou potentiel(le), causant un préjudice social ou économique

Note 1 à l'article: La fraude inclut également la falsification, la dissimulation, la destruction ou l'utilisation délibérées de documents falsifiés utilisés ou destinés à être utilisés à des fins commerciales, ou l'utilisation abusive d'informations ou d'une position à des fins d'enrichissement personnel.

Note 2 à l'article: Un comportement frauduleux ne constitue pas nécessairement une infraction à la loi.

Note 3 à l'article: La fraude peut impliquer un comportement frauduleux commis par des parties internes et/ou externes visant l'*organisme* (3.3) ou un comportement frauduleux commis par l'organisme lui-même visant des parties externes.

Note 4 à l'article: La fraude peut entraîner une perte d'argent ou d'autres biens pour des personnes internes ou externes à l'organisme, lorsqu'une tromperie est utilisée au moment même, immédiatement avant ou immédiatement après l'activité.

Note 5 à l'article: La fraude peut être externe, interne ou les deux. Une fraude externe est une fraude dont l'auteur n'est pas employé par l'organisme cible et n'a pas de lien étroit avec celui-ci. Une fraude interne est une fraude commise par au moins un auteur est employé par l'organisme cible ou entretient un lien étroit avec celui-ci, et dispose d'une connaissance approfondie de ses opérations, de ses systèmes et de ses procédures.

3.2
cas de fraude
acte de *fraude* (3.1) commise à l'encontre d'un *organisme* (3.3) ou par celui-ci

3.3
organisme
personne ou groupe de personnes ayant ses propres rôles (fonctions) avec des responsabilités, des autorités et des relations lui permettant d'atteindre ses *objectifs* (3.14)

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 associations 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 plus grande entité, le terme «organisme» fait uniquement référence à la partie de cette entité qui est comprise dans le champ d'application du *système de management anti-fraude* (3.11).

3.4
organisme cible
organisme (3.3) qui fait l'objet d'un *cas de fraude* (3.2)

3.5
partie intéressée
personne ou *organisme* (3.3) qui peut soit influer sur une décision ou une activité, soit être influencé ou s'estimer influencé par une décision ou une activité

3.6
direction
personne ou groupe de personnes qui oriente et dirige un *organisme* (3.3) 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 champ d'application du *système de management* (3.10) ne couvre qu'une partie de l'organisme, alors «direction» fait référence à ceux qui orientent et dirigent cette partie de l'organisme.

Note 3 à l'article: Les organismes peuvent être organisés en fonction du cadre légal dans lequel ils sont tenus d'opérer, ainsi que de leur taille, de leur secteur, etc. Certains organismes disposent à la fois d'un *organe de gouvernance* (3.7) et d'une *direction* (3.6), tandis que d'autres ne font pas la distinction des responsabilités entre plusieurs organes. Ces variantes, à la fois en matière d'organisme et de responsabilités, peuvent être prises en compte lors de l'application des exigences de l'Article 5.

3.7
organe de gouvernance
personne ou groupe de personnes assumant la redevabilité ultime pour l'ensemble de l'*organisme* (3.3)

Note 1 à l'article: Un organe de gouvernance peut être explicitement établi sous différentes formes, notamment, sans s'y limiter, un conseil d'administration, un conseil de surveillance, un directeur unique, une codirection ou des administrateurs.

Note 2 à l'article: Les normes de systèmes de management de l'ISO font référence au terme «direction» pour décrire un rôle qui, selon la norme et le contexte de l'organisme, rend compte à l'organe de gouvernance et est tenu redevable par ce dernier.

Note 3 à l'article: Tous les organismes, en particulier les petits et moyens organismes, ne disposent pas d'organe de gouvernance distinct de la direction. Dans ce cas, la direction joue le rôle d'organe de gouvernance.

[SOURCE: ISO 37000:2021, 3.3.4, modifié — Les notes à l'article ont été réorganisées: la Note 2 à l'article est maintenant la Note 1 à l'article; la Note 3 à l'article est maintenant la Note 2 à l'article; et la Note 3 à l'article a été ajoutée.]

3.8
personnel
directeurs, agents, employés, contractuels ou personnel intérimaire et bénévoles de l'*organisme* (3.3)

Note 1 à l'article: Différents types d'employés représentent différents types et degrés de *risque* (3.15) de fraude et peuvent être traités de manière différente dans le cadre de l'appréciation du risque de fraude et des modalités de gestion des risques de fraude de l'organisme.

[SOURCE: ISO 37001:2025, 3.24, modifié — La Note 1 a été modifiée et la Note 2 à l'article a été supprimée]

3.9
partenaire commercial
partie externe avec qui l'*organisme* (3.3) entretient, ou prévoit d'établir, une certaine forme de relation commerciale

Note 1 à l'article: Le partenaire commercial comprend notamment les clients, les entreprises communes, 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 vendeurs, les conseillers, les agents, les distributeurs, les représentants, les intermédiaires et les investisseurs. Cette définition est délibérément large et il convient qu'elle soit interprétée conformément au profil de *risque* (3.15) de fraude de l'organisme à appliquer aux partenaires commerciaux qui peuvent raisonnablement exposer l'organisme à des risques de fraude.

Note 2 à l'article: Différents types de partenaires commerciaux représentent différents types et degrés de risques de fraude. Un organisme disposera d'un degré d'influence différent pour les différents types de partenaires.

Note 3 à l'article: La référence au «métier» dans le présent document peut s'interpréter au sens large, c'est-à-dire comme les activités qui sont liées aux finalités de l'organisme.

[SOURCE: ISO 37001:2025, 3.25, modifié]

3.10
système de management
ensemble d'éléments corrélés ou en interaction d'un *organisme* (3.3), utilisés pour établir des *politiques* (3.12) et des *objectifs* (3.14), ainsi que des *processus* (3.18) 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.

3.11
système de management anti-fraude
FCMS
partie du *système de management* (3.10) destiné à maîtriser les risques de *fraude* (3.1) commise à l'encontre d'un *organisme* (3.3) ou par celui-ci

Note 1 à l'article: L'abréviation «FCMS» est dérivée du terme anglais développé correspondant «*fraud control management system*»

3.12
politique
intentions et orientations d'un *organisme* (3.3), telles qu'elles sont officiellement formulées par sa *direction* (3.6)

3.13
conflit d'intérêts
situation dans laquelle une partie intéressée a un intérêt personnel ou un intérêt organisationnel, direct ou indirect, qui peut compromettre ou interférer dans l'exercice impartial de sa capacité à agir dans le cadre de ses fonctions dans le meilleur intérêt de l'*organisme* (3.3)

Note 1 à l'article: Il peut exister différents types d'intérêts personnels: commerciaux, financiers, familiaux, professionnels, religieux ou politiques.

Note 2 à l'article: L'intérêt organisationnel concerne les intérêts d'un organisme ou d'une partie d'un organisme (par exemple une équipe ou un département) plutôt que ceux d'un individu.

[SOURCE: ISO 37009:20—[1)], 3.1.10]

3.14
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 l'éducation, la finance, la santé et la sécurité et l'environnement). Ils peuvent, par exemple, concerner tout l'organisme ou bien un projet, un produit ou un *processus* (3.18).

Note 3 à l'article: Il est possible qu'un objectif soit exprimé de différentes manières, par exemple par un résultat attendu, une finalité, un critère opérationnel, un objectif anti-fraude, ou par l'utilisation d'autres termes ayant la même signification (par exemple ambition, but ou cible).

Note 4 à l'article: Dans le contexte des *systèmes de management anti-fraude* (3.11), les objectifs anti-fraude sont fixés par l'*organisme* (3.3) en cohérence avec sa *politique* (3.12) anti-fraude et en vue d'obtenir des résultats précis.

3.15
risque
effet de l'incertitude sur les *objectifs* (3.14)

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 et à des conséquences également potentielles, 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.

3.16
niveau de risque
importance d'un *risque* (3.15) ou combinaison de risques, exprimée en termes de combinaison des conséquences et de leur vraisemblance

[SOURCE: ISO 37000:2021, 3.1.10]

3.17
appréciation du risque
ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque

[SOURCE: ISO 31073:2022, 3.3.8]

1) En cours d'élaboration. Stade au moment de la publication: ISO/DIS 37009:2024.

3.18
processus
ensemble d'activités corrélées ou en interaction qui utilise ou transforme des éléments d'entrée afin de produire un résultat

Note 1 à l'article: La désignation du résultat d'un processus comme «élément de sortie», «produit» ou «service» dépend du contexte de référence.

3.19
exigence
besoin ou attente formulé, généralement implicite ou obligatoire

Note 1 à l'article: «Généralement implicite» signifie qu'il est habituel ou courant, pour l'*organisme* (3.3) et les *parties intéressées* (3.5), que le besoin ou l'attente en question soit implicite.

Note 2 à l'article: Une exigence spécifiée est une exigence formulée, par exemple une *information documentée* (3.21).

3.20
compétence
aptitude à mettre en pratique des connaissances et des savoir-faire pour obtenir les résultats attendus

3.21
informations documentées
information devant être maîtrisée et tenue à jour par un *organisme* (3.3) 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* (3.10), y compris les *processus* (3.18) connexes;

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

— aux preuves des résultats atteints (enregistrements).

3.22
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats attendus (escomptés)

3.23
attaque
tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celui-ci

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.24
menace
cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un *organisme* (3.3)

[SOURCE: ISO/IEC 27000:2018, 3.74]