NORME INTERNATIONALE

ISO/IEC 27000

Redline version
compare la Cinquième édition
à la Quatrième édition

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Information technology — Security techniques — Information security management systems — Overview and vocabulary

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0e8c601-f195-40f9-82b8-57a028cf882d/iso-iec-27000-redline-2018

Numéro de référence
ISO/IEC 27000:redline:2018(F)

© ISO/IEC 2018

IMPORTANT — PLEASE NOTE

This is a mark-up copy and uses the following colour coding:

Text example 1 — indicates added text (in green)

~~Text example 2~~ — indicates removed text (in red)

— indicates added graphic figure

— indicates removed graphic figure

1.x ... — Heading numbers containg modifications are highlighted in yellow in the Table of Contents

DISCLAIMER

This Redline version provides you with a quick and easy way to compare the main changes between this edition of the standard and its previous edition. It doesn't capture all single changes such as punctuation but highlights the modifications providing customers with the most valuable information. Therefore it is important to note that this Redline version is not the official ISO standard and that the users must consult with the clean version of the standard, which is the official standard, for implementation purposes.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c28c601-f195-4b89-8b28-5ba02c988a4/iso-iec-27000-2018

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2018

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
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **v**

Introduction ..... **vi**

0.2 La famille de normes du SMSI vi

0.2 Objet du présent document vii

0.3 Objet de la présente Norme internationale vii

1 Domaine d'application **1**

2 Références normatives 1

~~2~~3 Termes et ~~définitions~~definitions **1**

~~3~~4 Systèmes de management de la sécurité de l'information **14**

~~3.1~~4.1 Généralités 14

~~3.2~~4.2 Qu'est-ce qu'un SMSI? 15

~~3.2.1~~4.2.1 Vue d'ensemble et principes 15

~~3.2.2~~4.2.2 L'information 16

~~3.2.3~~4.2.3 Sécurité de l'information 16

~~3.2.4~~4.2.4 Management 16

~~3.2.5~~4.2.5 Système de management 16

~~3.3~~4.3 Approche processus 17

~~3.4~~4.4 Raisons expliquant pourquoi un SMSI est important 17

~~3.5~~4.5 Établissement, surveillance, maintenance et amélioration d'un SMSI 18

~~3.5.1~~4.5.1 Vue d'ensemble 18

~~3.5.2~~4.5.2 Identifier les exigences liées à la sécurité de l'information 18

~~3.5.3~~4.5.3 Apprécier les risques liés à la sécurité de l'information 19

~~3.5.4~~4.5.4 Traiter les risques liés à la sécurité de l'information 19

~~3.5.5~~4.5.5 Sélectionner et mettre en œuvre les mesures de sécurité 20

~~3.5.6~~4.5.6 Surveiller, mettre à jour et améliorer l'efficacité du SMSI 21

~~3.5.7~~4.5.7 Amélioration continue 21

~~3.6~~4.6 Facteurs critiques de succès du SMSI 21

~~3.7~~4.7 Avantages de la famille de normes du SMSI 22

~~4~~5 La famille de normes du SMSI **22**

~~4.1~~5.1 ~~Information~~Informations générales 22

~~4.2~~5.2 ~~Normes~~Norme donnant une vue d'ensemble et décrivant la terminologie ISO/IEC 27000 (le présent document) 24

4.2.1 ISO/IEC 27000 (la présente Norme internationale) 24

~~4.3~~5.3 Normes spécifiant des exigences 24

~~4.3.1~~5.3.1 ~~ISO/IEC 27001~~ISO/IEC 27001 24

~~4.3.2~~5.3.2 ~~ISO/IEC 27006~~ISO/IEC 27006 25

5.3.3 ISO/IEC 27009 25

~~4.4~~5.4 Normes décrivant des lignes directrices générales 25

~~4.4.1~~5.4.1 ~~ISO/IEC 27002~~ISO/IEC 27002 25

~~4.4.2~~5.4.2 ~~ISO/IEC 27003~~ISO/IEC 27003 26

~~4.4.3~~5.4.3 ~~ISO/IEC 27004~~ISO/IEC 27004 26

~~4.4.4~~5.4.4 ~~ISO/IEC 27005~~ISO/IEC 27005 26

~~4.4.5~~5.4.5 ~~ISO/IEC 27007~~ISO/IEC 27007 26

~~4.4.6~~5.4.6 ~~ISO/IEC/TR 27008~~ISO/IEC TR 27008 27

~~4.4.7~~5.4.7 ~~ISO/IEC 27013~~ISO/IEC 27013 27

~~4.4.8~~5.4.8 ~~ISO/IEC 27014~~ISO/IEC 27014 27

~~4.4.9~~5.4.9 ~~ISO/IEC/TR 27016~~ISO/IEC TR 27016 28

5.4.10 ISO/IEC 27021 28

~~4.5~~5.5 Normes décrivant des lignes directrices propres à un secteur 28

~~4.5.1~~5.5.1 ~~ISO/IEC 27010~~ISO/IEC 27010 28

~~4.5.2~~5.5.2 ~~ISO/IEC 27011~~ISO/IEC 27011 29

4.5.3 ISO/IEC/TR 27015 29

~~4.5.4~~5.5.3 ~~ISO/IEC 27017~~ISO/IEC 27017 29

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c2e6601-f995-409-82b8-57528c8b2d19/iso-iec-27000-2018

~~4.5.5~~5.5.4 ~~ISO/IEC 27018~~ISO/IEC 27018 30
~~4.5.6~~5.5.5 ~~ISO/IEC/TR 27019~~ISO/IEC 27019 30
~~4.5.7~~5.5.6 ~~ISO 27799~~ISO 27799 31

~~**Annexe A** (informative) **Formes verbales utilisées pour exprimer des dispositions** ..... 32~~

~~**Annexe B** (informative) **Termes et propriété des termes** ..... 33~~

Bibliographie 39

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c28c601-f195-40f9-82b8-57a028cf882d/iso-iec-27000-2018

 © ISO/IEC 2018 – Tous droits réservés

Avant-propos

L'ISO (Organisation internationale de normalisation) ~~et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux~~est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO~~ ou de l'IEC participent à l'élaboration de Normes internationales par l'intermédiaire de comités techniques créés par l'organisme concerné pour traiter de domaines particuliers à une activité technique. Les~~). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO~~ et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux~~. 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 ~~et l'IEC~~ participent également aux travaux. ~~Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1~~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 ~~document~~documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir ~~http://www.iso.org/directives~~www.iso.org/directives).

~~L'attention est appelée~~L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire ~~l'objet~~l'objet de droits de propriété intellectuelle ou de droits analogues. ~~L'ISO~~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~~l'élaboration du document sont indiqués dans ~~l'Introduction~~l'Introduction et/ou dans la liste des déclarations de brevets reçues par ~~l'ISO~~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~~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'OMC~~l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: ~~Avant-propos — Informations supplémentaires~~www.iso.org/avant-propos.

Le ~~comité chargé de l'élaboration du présent document est l'ISO/~~présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, ~~sous-comité~~ SC 27, *Techniques de sécurité des technologies de l'information*.

Cette ~~quatrième~~cinquième édition annule et remplace la ~~troisième~~quatrième édition (ISO/IEC 27000:~~2014~~2016), qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

— modification du texte de l'Introduction;

— suppression de certains termes et définitions;

— alignement de l'Article 3 par rapport à la structure-cadre pour MSS;

— mise à jour de l'Article 5 pour refléter les modifications dans les normes concernées;

— suppression des Annexes A et B.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0a98c01-f9-
f89-82b8-37a08cf882d/iso-iec-27000-2018

Introduction

0.1 Vue d'ensemble

Les Normes internationales relatives aux systèmes de management fournissent un modèle en matière d'établissement et d'exploitation d'un système de management. Ce modèle comprend les caractéristiques que les experts dans le domaine s'accordent à reconnaître comme reflétant l'état de l'art au niveau international. Le sous-comité ISO/IEC JTC 1/SC 27 bénéficie de l'expérience d'un comité d'experts qui se consacre à l'élaboration des Normes internationales sur les systèmes de management pour la sécurité de l'information, connues également comme famille de normes du Système de Management de la Sécurité de l'Information (SMSI).

Grâce à l'utilisation de la famille de normes du SMSI, les organismes peuvent élaborer et mettre en œuvre un cadre de référence pour gérer la sécurité de leurs actifs informationnels, y compris les informations financières, la propriété intellectuelle, les informations sur les employés, ou les informations qui leur sont confiées par des clients ou des tiers. Ils peuvent également utiliser ces normes pour se préparer à une évaluation indépendante de leur SMSI en matière de protection de l'information.

~~0.2 La famille de normes du SMSI~~

~~La famille de normes du SMSI (voir Article 4) a pour objet d'aider les organismes de tous types et de toutes tailles à déployer et à exploiter un SMSI. Elle se compose des Normes internationales suivantes (indiquées ci-dessous par ordre numérique) regroupées sous le titre général *Technologies de l'information — Techniques de sécurité*.~~

- ~~ISO/IEC 27000, *Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*~~
- ~~ISO/IEC 27001, *Systèmes de management de la sécurité de l'information — Exigences*~~
- ~~ISO/IEC 27002, *Code de bonnes pratiques pour le management de la sécurité de l'information*~~
- ~~ISO/IEC 27003, *Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information*~~
- ~~ISO/IEC 27004, *Management de la sécurité de l'information — Mesurage*~~
- ~~ISO/IEC 27005, *Gestion des risques liés à la sécurité de l'information*~~
- ~~ISO/IEC 27006, *Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*~~
- ~~ISO/IEC 27007, *Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information*~~
- ~~ISO/IEC/TR 27008, *Lignes directrices pour les auditeurs des contrôles de sécurité de l'information*~~
- ~~ISO/IEC 27009, *Application de l'ISO/IEC 27001 à un secteur spécifique — Exigences*~~
- ~~ISO/IEC 27010, *Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles*~~
- ~~ISO/IEC 27011, *Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002*~~
- ~~ISO/IEC 27013, *Guide sur la mise en œuvre intégrée de l'ISO/IEC 27001 et ISO/IEC 20000-1*~~
- ~~ISO/IEC 27014, *Gouvernance de la sécurité de l'information*~~
- ~~ISO/IEC/TR 27015, *Lignes directrices pour le management de la sécurité de l'information pour les services financiers*~~
- ~~ISO/IEC/TR 27016, *Management de la sécurité de l'information — Économie organisationnelle*~~

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/0c2b3e91-81ce-40be-82b8-57a228cf02d/iso-iec-27000-2018

 © ISO/IEC 2018 – Tous droits réservés

— ISO/IEC 27017, *Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'*ISO/IEC 27002 *pour les services du nuage*

— ISO/IEC 27018, *Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

— ISO/IEC 27019, *Lignes directrices de management de la sécurité de l'information fondées sur l'*ISO/IEC 27002 *pour les systèmes de contrôle des processus spécifiques à l'industrie de l'énergie*

NOTE Le titre général « *Technologies de l'information — Techniques de sécurité* » indique que ces Normes internationales ont été élaborées par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Les Normes internationales qui font également partie de la famille de normes du SMSI, mais qui ne sont pas regroupées sous le même titre général, sont les suivantes:

— ISO 27799, *Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'*ISO/IEC 27002

0.2 Objet du présent document

La famille de normes du SMSI comporte des normes qui:

a) définissent les exigences relatives à un SMSI et à ceux qui certifient de tels systèmes;

b) apportent des informations directes, des recommandations et/ou une interprétation détaillées concernant le processus général visant à établir, mettre en œuvre, maintenir et améliorer un SMSI;

c) présentent des lignes directrices propres à des secteurs particuliers en matière de SMSI;

d) traitent de l'évaluation de la conformité d'un SMSI.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0b58c601-f195-40b5-8268-57a0c8ec882d/iso-iec-27000-2018

0.3 Objet de la présente Norme internationale

La présente Norme internationale offre un aperçu d'ensemble des systèmes de management de la sécurité de l'information et définit les termes qui s'y rapportent.

NOTE L'Annexe A fournit des éclaircissements sur la façon dont les formes verbales sont utilisées pour exprimer des exigences et/ou des préconisations dans la famille de normes du SMSI.

La famille de normes du SMSI comporte des normes qui:

a) définissent les exigences relatives à un SMSI et à ceux qui certifient de tels systèmes;

b) apportent des informations directes, des préconisations et/ou une interprétation détaillées concernant le processus général visant à établir, mettre en œuvre, maintenir et améliorer un SMSI;

c) présentent des lignes directrices propres à des secteurs particuliers en matière de SMSI;

d) traitent de l'évaluation de la conformité d'un SMSI.

Les termes et les définitions fournis dans la présente Norme internationale:

— couvrent les termes et les définitions d'usage courant dans la famille de normes du SMSI;

— ne couvrent pas l'ensemble des termes et des définitions utilisés dans la famille de normes du SMSI;

— ne limitent pas la famille de normes du SMSI en définissant de nouveaux termes à utiliser.

0.3 Contenu du présent document

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

— «doit» indique une exigence;

— «il convient» indique une recommandation;

— «peut» indique une autorisation («may» en anglais),

— ou une possibilité ou une capacité («can» en anglais).

Les informations sous forme de «NOTE» sont fournies pour clarifier l'exigence associée ou en faciliter la compréhension. Les «Notes à l'article» employées à l'Article 3 fournissent des informations supplémentaires qui viennent compléter les données terminologiques et peuvent contenir des dispositions concernant l'usage d'un terme.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c28c601-f195-40f9-82b8-57a028cf882d/iso-iec-27000-2018

 © ISO/IEC ISO pub-date year – Tous droits réservés

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

1 Domaine d'application

~~La présente Norme internationale offre une vue d'ensemble des systèmes de management de la sécurité de l'information, ainsi que des termes et définitions d'usage courant dans la famille de normes du SMSI. La présente Norme internationale est applicable à tous les types et à toutes les tailles d'organismes (par exemple: les entreprises commerciales, les organismes publics, les organismes à but non lucratif).~~

Le présent document offre une vue d'ensemble des systèmes de management de la sécurité de l'information (SMSI). Il comprend également les termes et définitions d'usage courant dans la famille de normes du SMSI. Le présent document est applicable à tous les types et à toutes les tailles d'organismes (par exemple: les entreprises commerciales, les organismes publics, les organismes à but non lucratif).

Les termes et les définitions fournis dans le présent document:

— couvrent les termes et les définitions d'usage courant dans la famille de normes du SMSI;

— ne couvrent pas l'ensemble des termes et des définitions utilisés dans la famille de normes du SMSI;

— ne limitent pas la famille de normes du SMSI en définissant de nouveaux termes à utiliser.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c2e4501-f195-4012-92b8-57a1a28cf882d/iso-iec-27000-2018

2 Références normatives

Le présent document ne contient aucune référence normative.

~~2~~3 Termes et ~~définitions~~ definitions

~~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~~3.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les *exigences* (~~2.63~~3.56) propres à la sécurité et à l'activité métier

~~**3.2**~~
~~**modèle analytique**~~
~~algorithme ou calcul combinant une ou plusieurs *mesures élémentaires* (2.10) et/ou *mesures dérivées (2.22)* avec les *critères de décision* associés (2.21)~~

~~3.3~~3.2
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

~~**2.4**~~
~~**attribut**~~
~~propriété ou caractéristique d'un *objet* (2.55) qui peut être distingué quantitativement ou qualitativement par des moyens humains ou automatiques~~

~~[SOURCE: ISO/IEC 15939:2007, 2.2, modifiée — Le terme « entité » a été remplacé par « objet » dans la définition.]~~

~~**2.5**~~**3.3**
audit
processus (2.61)*processus* méthodique, indépendant et documenté (3.54) 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 (audit de première partie), externe (audit de seconde ou de tierce partie) ou combiné (associant deux disciplines 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.

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

~~**2.6**~~**3.4**
champ de l'audit
étendue et limites d'un *audit* (~~2.5~~3.3)

[SOURCE: ISO 19011:2011, 3.14, modifiée — Suppression de la note 1 à l'article.]

~~**2.7**~~**3.5**
authentification
méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correcte

~~**2.8**~~**3.6**
authenticité
propriété selon laquelle une entité est ce qu'elle revendique être

~~**2.9**~~**3.7**
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

~~**2.10**~~**3.8**
mesure élémentaire
mesure (~~2.47~~3.42) définie en fonction d'un ~~*attribut* (2.4)~~attribut et de la méthode de mesurage spécifiée pour le quantifier

~~[SOURCE: ISO/IEC 15939:2007, 2.3, modifiée — Suppression de la note 2 à l'article.]~~

Note 1 à l'article: Une mesure élémentaire est fonctionnellement indépendante des autres ~~*mesures* (2.47)~~mesures.

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modifiée — Suppression de la note 2 à l'article.]

~~**2.11**~~**3.9**
compétence
capacité à appliquer des connaissances et des aptitudes pour obtenir les résultats escomptés

~~**2.12**~~**3.10**
confidentialité
propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des *processus* (~~2.61~~3.54) non autorisés

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9c28c601-f195-40f9-82b5-57a028cf882e/iso-iec-27000-2018

 © ISO/IEC 2018 – Tous droits réservés

~~2.13~~3.11
conformité
satisfaction d'une *exigence* (~~2.63~~3.56)

~~Note 1 à l'article: Le terme anglais « conformance » est un synonyme, mais il est déconseillé.~~

~~2.14~~3.12
conséquence
effet d'un *événement* (~~2.25~~3.21) affectant les *objectifs* (~~2.56~~3.49)

~~[SOURCE: Guide ISO 73:2009, 3.6.1.3, modifié]~~

Note 1 à l'article: Un ~~*événement* (2.25)~~événement peut ~~entraîner~~ engendrer une série de conséquences.

Note 2 à l'article: Une conséquence peut être certaine ou incertaine~~. Dans~~; dans le contexte de la ~~*sécurité de l'information* (2.33)~~sécurité de l'information, elle est généralement négative.

Note 3 à l'article: Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 4 à l'article: Des conséquences initiales peuvent déclencher des réactions en chaîne.

[SOURCE: Guide ISO 73:2009, 3.6.1.3, modifié — Modification de la Note 2 à l'article après «et».]

~~2.15~~3.13
amélioration continue
activité régulière destinée à améliorer les *performances* (~~2.59~~3.52)

~~2.16~~3.14
mesure de sécurité
mesure qui modifie un *risque* (~~2.68~~3.61)

~~[SOURCE: Guide ISO 73:2009, 3.8.1.1]~~

Note 1 à l'article: Les mesures de sécurité comprennent tous les *processus* (~~2.61~~3.54), *politiques* (~~2.60~~3.53), dispositifs, pratiques ou autres actions qui modifient un *risque* (~~2.68~~3.61).

Note 2 à l'article: ~~Les~~Il est possible que les mesures de sécurité ne ~~peuvent~~puissent pas toujours aboutir à la modification voulue ou supposée.

[SOURCE: Guide ISO 73:2009, 3.8.1.1, — Modification de la Note 2 à l'article.]

~~2.17~~3.15
objectif ~~d'une~~ d'une mesure de sécurité
déclaration décrivant ce qui est attendu de la mise en œuvre des *mesures de sécurité* (~~2.16~~3.14)

~~2.18~~3.16
correction
action visant à éliminer une *non-conformité* (~~2.53~~3.47) détectée

~~2.19~~3.17
action corrective
action visant à éliminer la cause d'une *non-conformité* (~~2.53~~3.47) et à empêcher qu'elle ne se répète

~~**2.20**~~
~~**données**~~
~~ensemble des valeurs attribuées aux *mesures élémentaires* (2.10), *mesures dérivées* (2.22) et/ou aux *indicateurs* (2.30)~~

~~[SOURCE: ISO/IEC 15939:2007, 2.4, modifiée — Ajout de la note 1 à l'article.]~~

~~Note 1 à l'article: Cette définition s'applique uniquement dans le contexte de l'ISO/IEC 27004.~~

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c2b5601-f195-4019-92b8-5a028cf882d/iso-iec-27000-2018

~~**2.21**~~
~~**critères de décision**~~
~~seuils, cibles ou modèles utilisés pour déterminer la nécessité d'une action ou d'un complément d'enquête, ou pour décrire le niveau de confiance dans un résultat donné~~

~~[SOURCE: ISO/IEC 15939:2007, 2.7]~~

~~**2.22**~~**3.18**
mesure dérivée
mesure (~~2.47~~3.42) définie en fonction d'au moins deux *mesures élémentaires* (~~2.10~~3.8)

[SOURCE: ISO/IEC/IEEE 15939:~~2007, 2.8~~2017, 3.8, modifiée — Suppression de la note 1 à l'article.]

~~**2.23**~~**3.19**
informations documentées
informations devant être contrôlées et mises à jour par un *organisme* (~~2.57~~3.50) et le support sur lequel elles sont stockées

Note 1 à l'article: Les informations documentées peuvent être dans n'importe quel format, sur n'importe quel support et provenir de n'importe quelle source.

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

— au *système de management* (~~2.46~~3.41) et aux *processus* (2.61)*processus* associés (3.54);

— aux informations créées pour permettre à l'*organisme* (~~2.57~~3.50) de fonctionner (documentation);

— aux preuves des résultats obtenus (enregistrements).

~~**2.24**~~**3.20**
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

~~**2.25**~~**3.21**
événement
occurrence ou changement d'un ensemble particulier de circonstances

~~[SOURCE: Guide ISO 73:2009, 3.5.1.3, modifié — Suppression de la note 4 à l'article.]~~

Note 1 à l'article: Un événement peut être unique ou se reproduire. Il peut avoir plusieurs causes.

Note 2 à l'article: Un événement peut consister en quelque chose qui ne se produit pas.

Note 3 à l'article: Un événement peut parfois être qualifié «d'incident» ou «d'accident».

[SOURCE: Guide ISO 73:2009, 3.5.1.3, modifié — Suppression de la note 4 à l'article.]

~~**2.26**~~
~~**management exécutif**~~
~~personne ou groupe de personnes ayant reçu des *instances dirigeantes* (2.29) la responsabilité de la mise en œuvre des stratégies et politiques afin d'atteindre les objectifs de l'*organisme* (2.57)~~

~~Note 1 à l'article: Le management exécutif est parfois appelé la *direction* (2.84). Il peut comprendre les présidents directeurs généraux, les directeurs financiers, les directeurs des systèmes d'information et autres fonctions similaires.~~

~~**2.27**~~**3.22**
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses *objectifs* (~~2.56~~3.49)

Note 1 à l'article: Le contexte externe peut inclure les aspects suivants:

— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local;

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0c2e6011-2e05-4019-8218-57a028cf882d/iso-iec-27000-2018

 © ISO/IEC 2018 – Tous droits réservés

— *les facteurs clés et tendances ayant un impact déterminant sur les objectifs* de l'organisme (3.50);

— les relations avec les *parties prenantes* (3.37) externes, les perceptions et valeurs relatives à celles-ci.

[SOURCE: Guide ISO 73:2009, 3.3.1.1]

~~Note 2 à l'article: Le contexte externe peut inclure les aspects suivants:~~

~~— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local;~~

~~— les facteurs clés et tendances ayant un impact déterminant sur les *objectifs* (2.56) de l'*organisme* (2.57);~~

~~— les relations avec les *parties prenantes* (2.82) externes, les perceptions et valeurs relatives à celles-ci.~~

~~2.28~~3.23
gouvernance de la sécurité de l'information
système par lequel un *organisme* (~~2.57~~3.50) conduit et supervise les activités liées à la *sécurité de l'information* (~~2.33~~3.28)

~~2.29~~3.24
instances dirigeantes
personne ou groupe de personnes ayant la responsabilité des *performances* (~~2.59~~3.52) et de la conformité de l'*organisme* (~~2.57~~3.50)

Note 1 à l'article: Dans certaines juridictions, les instances dirigeantes peuvent être constituées d'un conseil d'administration.

~~2.30~~3.25
indicateur
mesure (~~2.47~~3.42) qui fournit une estimation ou une évaluation ~~des *attributs* (2.4) spécifiés à partir d'un *modèle analytique* (2.2) concernant les *besoins d'information* (2.31) définis~~

~~2.31~~3.26
besoin d'information
information nécessaire pour gérer les *objectifs* (~~2.56~~3.49), les buts, les risques et les problèmes

[SOURCE: ISO/IEC/IEEE 15939:~~2007, 2.12~~2017, 3.12]

~~2.32~~3.27
moyens de traitement de l'information
tout système, service ou infrastructure de traitement de l'information, ou le local les abritant

~~2.33~~3.28
sécurité de l'information
protection de la *confidentialité* (~~2.12~~3.10), de l'*intégrité* (~~2.40~~3.36) et de la *disponibilité* (~~2.9~~3.7) de l'information

Note 1 à l'article: En outre, d'autres propriétés, telles que ~~l'*authenticité (2.8*~~*l'authenticité* (3.6), l'imputabilité, la *non-répudiation* (~~2.54~~3.48) et la *fiabilité* (~~2.62~~3.55) peuvent également être concernées.

~~2.34~~3.29
continuité de la sécurité de l'information
processus (~~2.61~~3.54) et procédures visant à assurer la continuité des opérations liées à la *sécurité de l'information* (~~2.33~~3.28)

~~2.35~~3.30
événement lié à la sécurité de l'information
occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la *politique* (~~2.60~~3.28) de sécurité de l'~~*sécurité de l'information (2.33*~~*information* (3.53) ou un échec des *mesures de sécurité* (~~2.16~~3.14), ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/0c28c001-f195-4a3-82b-57a028cf882/iso-iec-27000-2018