NORME INTERNATIONALE

ISO/IEC 27005

Quatrième édition
2022-10

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

Numéro de référence
ISO/IEC 27005:2022(F)

© ISO/IEC 2022

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2022

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
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

© ISO/IEC 2022 – Tous droits réservés

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

© ISO/IEC 2022 – 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 membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

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 ou www.iec.ch/members_experts/refdocs).

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 et l'IEC ne sauraient être tenues pour responsables 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) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.ch).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71ed98fbe1e1/iso-iec-27005-2022

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette quatrième édition annule et remplace la troisième édition (ISO/IEC 27005:2018), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— toutes les recommandations ont été alignées sur l'ISO/IEC 27001:2022 et sur l'ISO 31000:2018;

— la terminologie a été alignée sur celle de l'ISO 31000:2018;

— la structure des articles et paragraphes a été ajustée selon la mise en page de l'ISO/IEC 27001:2022;

— des concepts de scénario de risque ont été ajoutés;

— une distinction est faite entre l'approche basée sur les événements et l'approche basée sur les biens en matière d'identification des risques;

— le contenu des annexes a été révisé et réorganisé au sein d'une seule annexe.

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 et www.iec.ch/national-committees.

© ISO/IEC 2022 – Tous droits réservés

Introduction

Le présent document fournit des recommandations concernant:

— la mise en œuvre des exigences en matière de risques liés à la sécurité de l'information spécifiées dans l'ISO/IEC 27001;

— les références essentielles incluses dans les normes développées par l'ISO/IEC JTC 1/SC 27 concernant les activités de gestion des risques liés à la sécurité de l'information;

— les actions qui traitent des risques liés à la sécurité de l'information (voir l'ISO/IEC 27001:2022, 6.1 et Article 8);

— la mise en œuvre des recommandations en matière de gestion des risques de l'ISO 31000 dans le contexte de la sécurité de l'information.

Le présent document contient des recommandations détaillées concernant la gestion des risques et complète les recommandations de l'ISO/IEC 27003.

Le présent document est conçu pour être utilisé par les entités suivantes:

— les organismes qui prévoient d'établir et de mettre en œuvre un système de gestion de la sécurité de l'information conformément à l'ISO/IEC 27001;

— les personnes chargées de la gestion des risques liés à la sécurité de l'information ou impliquées dans celle-ci (par exemple les personnes spécialisées dans la gestion de ces risques, les propriétaires du risque et les autres parties intéressées);

— les organismes qui ont l'intention d'améliorer leur processus de gestion des risques liés à la sécurité de l'information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

© ISO/IEC 2022 – Tous droits réservés

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

1 Domaine d'application

Le présent document fournit des recommandations pour aider les organismes à:

— satisfaire aux exigences de l'ISO/IEC 27001 concernant les actions visant à traiter les risques liés à la sécurité de l'information;

— réaliser des activités de gestion des risques liés à la sécurité de l'information, en particulier l'appréciation et le traitement de ces risques.

Le présent document est applicable à tous les organismes, quels que soient leur type, leur taille ou leur secteur.

2 Références normatives

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 27000 ainsi que les 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 Termes associés aux risques liés à la sécurité de l'information

3.1.1
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses objectifs

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

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

— les facteurs et tendances clés ayant une incidence sur les objectifs de l'organisme;

— les relations avec les parties intéressées externes, leurs perceptions, leurs valeurs, leurs besoins et leurs attentes;

© ISO/IEC 2022 – Tous droits réservés

— les relations contractuelles et les engagements;

— la complexité des réseaux et des dépendances.

[SOURCE: Guide ISO 73:2009, 3.3.1.1, modifié — La Note 1 à l'article a été modifiée.]

3.1.2
contexte interne
environnement interne dans lequel l'organisme cherche à atteindre ses objectifs

Note 1 à l'article: Le contexte interne peut comprendre:

— la vision, la mission et les valeurs;

— la gouvernance, l'organisation, les rôles et responsabilités;

— la stratégie, les objectifs et les politiques;

— la culture de l'organisme;

— les normes, les lignes directrices et les modèles adoptés par l'organisme;

— les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnel, processus, systèmes et technologies);

— les données, les systèmes d'information et la circulation de l'information;

— les relations avec les parties intéressées internes, en tenant compte de leurs perceptions et de leurs valeurs;

— les relations contractuelles et les engagements;

— les interdépendances et les interconnexions internes.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: Guide ISO 73:2009, 3.3.1.2, modifié — La Note 1 à l'article a été modifiée.]

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

3.1.3
risque
effet de l'incertitude sur les objectifs

Note 1 à l'article: Un effet est un écart, positif ou négatif, par rapport à un attendu.

Note 2 à l'article: Les objectifs peuvent avoir différents aspects, être de catégories différentes, et peuvent concerner différents niveaux.

Note 3 à l'article: L'incertitude est l'état, même partiel, de manque d'information qui entrave la compréhension ou la connaissance d'un *événement* (3.1.11), de ses *conséquences* (3.1.14) ou de sa *vraisemblance* (3.1.13).

Note 4 à l'article: Un risque est généralement exprimé en termes de *sources de risque* (3.1.6), événements potentiels avec leurs conséquences et leur vraisemblance.

Note 5 à l'article: Dans le contexte des systèmes de gestion de la sécurité de l'information, les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.

Note 6 à l'article: Les risques liés à la sécurité de l'information sont généralement associés à un effet négatif de l'incertitude sur les objectifs de sécurité de l'information.

Note 7 à l'article: Le risque de sécurité de l'information peut être associé à la possibilité que des *menaces* (3.1.9) exploitent les *vulnérabilités* (3.1.10) d'un bien informationnel ou d'un groupe de biens informationnels et portent ainsi un préjudice à un organisme.

[SOURCE: ISO 31000:2018, 3.1, modifié — La phrase «Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces» a été remplacée par «positif ou négatif» dans la Note 1 à l'article; la Note 3 à l'article a été renumérotée en Note 4 à l'article; et les Notes 3, 5, 6 et 7 à l'article ont été ajoutées.]

© ISO/IEC 2022 – Tous droits réservés

3.1.4
scénario de risque
séquence ou combinaison d'*événements* (3.1.11) qui conduisent de la cause initiale à la *conséquence* indésirable (3.1.14)

[SOURCE: ISO 17666:2016, 3.1.13, modifié — La Note 1 à l'article a été supprimée.]

3.1.5
propriétaire du risque
personne ou entité ayant la responsabilité du *risque* (3.1.3) et ayant autorité pour le gérer

[SOURCE: Guide ISO 73:2009, 3.5.1.5]

3.1.6
source de risque
tout élément qui, seul ou combiné à d'autres, est susceptible d'engendrer un *risque* (3.1.3)

Note 1 à l'article: Une source de risque peut être de l'un de ces trois types:

— humain;

— environnemental;

— technique.

Note 2 à l'article: Une source de risque de type humain peut être volontaire ou involontaire.

[SOURCE: ISO 31000:2018, 3.4, modifié — Les Notes 1 et 2 à l'article ont été ajoutées.]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.7
critères de risque
termes de référence vis-à-vis desquels l'importance d'un *risque* (3.1.3) est évalué

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a01e5455-415d-48cd-9a5e-71cd98fbe1e1/iso-iec-27005-2022

Note 1 à l'article: Les critères de risque sont fondés sur les objectifs de l'organisme ainsi que sur le *contexte externe* (3.1.1) et *interne* (3.1.2).

Note 2 à l'article: Les critères de risque peuvent être issus de normes, de lois, de politiques et d'autres exigences.

[SOURCE: Guide ISO 73:2009, 3.3.1.3]

3.1.8
goût du risque
importance et type de *risque* (3.1.3) qu'un organisme est prêt à saisir ou à préserver

[SOURCE: Guide ISO 73:2009, 3.7.1.2]

3.1.9
menace
cause potentielle d'un *incident lié à la sécurité de l'information* (3.1.12) qui peut entraîner des dommages pour un système ou porter préjudice à un organisme

3.1.10
vulnérabilité
faille dans un bien ou dans un *moyen de maîtrise* (3.1.16) qui peut être exploitée de sorte qu'un *événement* (3.1.11) ayant une *conséquence* (3.1.14) négative se produise

3.1.11
événement
occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article: Un événement peut être unique ou se reproduire et peut avoir plusieurs causes et plusieurs *conséquences* (3.1.14).

© ISO/IEC 2022 – Tous droits réservés

Note 2 à l'article: Un événement peut être quelque chose qui est attendu, mais qui ne se produit pas, ou quelque chose auquel on ne s'attend pas, mais qui se produit.

[SOURCE: ISO 31000:2018, 3.5, modifié — La Note 3 à l'article a été supprimée.]

3.1.12
incident lié à la sécurité de l'information
un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information

3.1.13
vraisemblance
possibilité que quelque chose se produise

Note 1 à l'article: Dans la terminologie de la gestion des risques, le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article: Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie de la gestion des risques, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: ISO 31000:2018, 3.7]

3.1.14
conséquence
effet d'un *événement* (3.1.11) affectant les objectifs

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/...
...71ed98fbe1e1/iso-iec-27005-2022

Note 1 à l'article: Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs, directs ou indirects, sur l'atteinte des objectifs.

Note 2 à l'article: Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 3 à l'article: Toute conséquence peut déclencher des effets en cascade et cumulatifs.

[SOURCE: ISO 31000:2018, 3.6]

3.1.15
niveau de risque
importance d'un *risque* (3.1.3) exprimée en termes de combinaison des *conséquences* (3.1.14) et de leur *vraisemblance* (3.1.13)

[SOURCE: Guide ISO 73:2009, 3.6.1.8, modifié — «importance d'un risque ou combinaison de risques» a été remplacé par «importance d'un risque».]

3.1.16
moyen de maîtrise
action qui maintient et/ou modifie un *risque* (3.1.3)

Note 1 à l'article: Un moyen de maîtrise inclut, sans toutefois s'y limiter, n'importe quels processus, politique, dispositif, pratique ou autres conditions et/ou actions qui maintiennent et/ou modifient un risque.

Note 2 à l'article: Un moyen de maîtrise n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

[SOURCE: ISO 31000:2018, 3.8]

© ISO/IEC 2022 – Tous droits réservés

3.1.17
risque résiduel
risque (3.1.3) subsistant après le *traitement du risque* (3.2.7)

Note 1 à l'article: Un risque résiduel peut inclure un risque non identifié.

Note 2 à l'article: Les risques résiduels peuvent également inclure des risques pris.

[SOURCE: Guide ISO 73:2009, 3.8.1.6, modifié — La Note 2 à l'article a été modifiée.]

3.2 Termes relatifs à la gestion des risques liés à la sécurité de l'information

3.2.1
processus de management du risque
application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des *risques* (3.1.3)

[SOURCE: Guide ISO 73:2009, 3.1]

3.2.2
communication et concertation relatives au risque
ensemble de processus itératifs et continus mis en œuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les parties intéressées concernant la gestion des *risques* (3.1.3)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Note 1 à l'article: Ces informations peuvent concerner l'existence, la nature, la forme, la *vraisemblance* (3.1.13), l'importance, l'évaluation, l'acceptation et le traitement du risque

Note 2 à l'article: La concertation est un processus de communication argumentée à double sens entre un organisme et ses parties intéressées, sur une question donnée avant de prendre une décision ou de déterminer une orientation concernant ladite question. La concertation est:

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-7fcd981be1e1/iso-iec-27005-2022

— un processus dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir;

— une contribution à une prise de décision, et non une prise de décision conjointe.

3.2.3
appréciation du risque
ensemble du processus d'*identification des risques* (3.2.4), d'*analyse du risque* (3.2.5) et d'*évaluation du risque* (3.2.6)

[SOURCE: Guide ISO 73:2009, 3.4.1]

3.2.4
identification des risques
processus de recherche, de reconnaissance et de description des *risques* (3.1.3)

Note 1 à l'article: L'identification des risques comprend l'identification des *sources de risque* (3.1.6), des *événements* (3.1.11), de leurs causes et de leurs *conséquences* (3.1.14) potentielles.

Note 2 à l'article: L'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des parties intéressées.

[SOURCE: Guide ISO 73:2009, 3.5.1, modifié — «parties intéressées» a remplacé «parties prenantes» dans la Note 2 à l'article.]

© ISO/IEC 2022 – Tous droits réservés

3.2.5
analyse du risque
processus mis en œuvre pour comprendre la nature d'un *risque* (3.1.3) et pour déterminer le *niveau de risque* (3.1.15)

Note 1 à l'article: L'analyse du risque fournit la base de l'*évaluation du risque* (3.2.6) et les décisions relatives au *traitement du risque* (3.2.7).

Note 2 à l'article: L'analyse du risque inclut l'estimation du risque.

[SOURCE: Guide ISO 73:2009, 3.6.1]

3.2.6
évaluation du risque
processus de comparaison des résultats de l'*analyse du risque* (3.2.5) avec les *critères de risque* (3.1.7) afin de déterminer si le *risque* (3.1.3) et/ou son importance sont acceptables ou tolérables

Note 1 à l'article: L'évaluation du risque aide à la prise de décision relative au *traitement du risque* (3.2.7).

[SOURCE: Guide ISO 73:2009, 3.7.1, modifié — «importance» a remplacé «importance».]

3.2.7
traitement du risque
processus destiné à modifier un *risque* (3.1.3)

Note 1 à l'article: Le traitement du risque peut inclure:

— un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque;

— la prise ou l'augmentation d'un risque afin de saisir une opportunité;

— l'élimination de la *source de risque* (3.1.6);

— une modification de la *vraisemblance* (3.1.13);

— une modification des *conséquences* (3.1.14);

— un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque); et

— une prise de risque fondée sur une décision argumentée.

Note 2 à l'article: Le traitement du risque lié à la sécurité de l'information n'inclut pas la «prise ou l'augmentation d'un risque afin de saisir une opportunité», mais l'organisme peut avoir cette possibilité dans le cadre général de la gestion des risques.

Note 3 à l'article: Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

Note 4 à l'article: Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

[SOURCE: Guide ISO 73:2009, 3.8.1, modifié — La Note 1 à l'article a été ajoutée et les Notes 1 et 2 à l'article présentes dans le document d'origine ont été renumérotées en Notes 2 et 3 à l'article.]

3.2.8
acceptation du risque
décision argumentée en faveur de la prise d'un *risque* (3.1.3) particulier

Note 1 à l'article: L'acceptation du risque peut avoir lieu sans *traitement du risque* (3.2.7) ou au cours du processus de traitement du risque.

Note 2 à l'article: Les risques acceptés font l'objet d'une surveillance et d'une revue.

[SOURCE: Guide ISO 73:2009, 3.7.1.6]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-8fbe1e1/iso-iec-27005-2022

© ISO/IEC 2022 – Tous droits réservés

3.2.9
partage du risque
forme de *traitement du risque* (3.2.7) impliquant la répartition consentie du *risque* (3.1.3) avec d'autres parties

Note 1 à l'article: Des obligations légales ou réglementaires peuvent limiter, interdire ou imposer le partage du risque.

Note 2 à l'article: Le partage du risque peut intervenir sous forme d'assurances ou autres types de contrats.

Note 3 à l'article: Le degré de répartition du risque peut dépendre de la fiabilité et de la clarté des dispositions prises pour le partage.

Note 4 à l'article: Le transfert du risque est une forme de partage du risque.

[SOURCE: Guide ISO 73:2009, 3.8.1.3]

3.2.10
prise de risque
acceptation temporaire de l'avantage potentiel d'un gain ou de la charge potentielle d'une perte découlant d'un *risque* (3.1.3) particulier

Note 1 à l'article: La prise de risque peut être limitée à une certaine période.

Note 2 à l'article: Le *niveau de risque* (3.1.15) pris peut dépendre des *critères de risque* (3.1.7).

[SOURCE: Guide ISO 73:2009, 3.8.1.5, modifié — Le mot «temporaire» a été ajouté au début de la définition et la phrase «La prise de risque comprend l'acceptation des risques résiduels» a été remplacée par «La prise de risque peut être limitée à une certaine période» dans la Note 1 à l'article.]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4 Structure du présent document

ISO/IEC 27005:2022
https://standards.iteh.ai/catalog/standards/sist/a81e3455-413d-48cd-9a3c-71cd98fbe1e1/iso-iec-27005-2022

Le présent document est structuré comme suit:

— Article 5: Gestion des risques liés à la sécurité de l'information;

— Article 6: Établissement du contexte;

— Article 7: Processus d'appréciation du risque lié à la sécurité de l'information;

— Article 8: Processus de traitement du risque lié à la sécurité de l'information;

— Article 9: Réalisation des activités opérationnelles;

— Article 10: Exploiter les processus SMSI connexes.

À l'exception des descriptions fournies dans les articles et paragraphes généraux, toutes les activités liées à la gestion des risques, présentées dans les Articles 7 à 10, sont structurées de la manière suivante:

Élément d'entrée: Identifie les informations requises pour réaliser l'activité.

Action: Décrit l'activité.

Déclencheur: Propose des recommandations quant au moment auquel l'activité doit débuter, par exemple en raison d'un changement au sein de l'organisme ou conformément à un plan, ou en raison d'un changement dans le contexte externe de l'organisme.

Élément de sortie: Identifie les informations obtenues après la réalisation de l'activité, ainsi que les critères qu'il convient de satisfaire.

Recommandations: Propose des recommandations sur la réalisation de l'activité, le mot clé et le concept clé.

© ISO/IEC 2022 – Tous droits réservés

5 Gestion des risques liés à la sécurité de l'information

5.1 Processus de gestion des risques liés à la sécurité de l'information

Le processus de gestion des risques liés à la sécurité de l'information est présenté à la Figure 1.

NOTE Ce processus est identique au processus général de gestion des risques décrit dans l'ISO 31000.

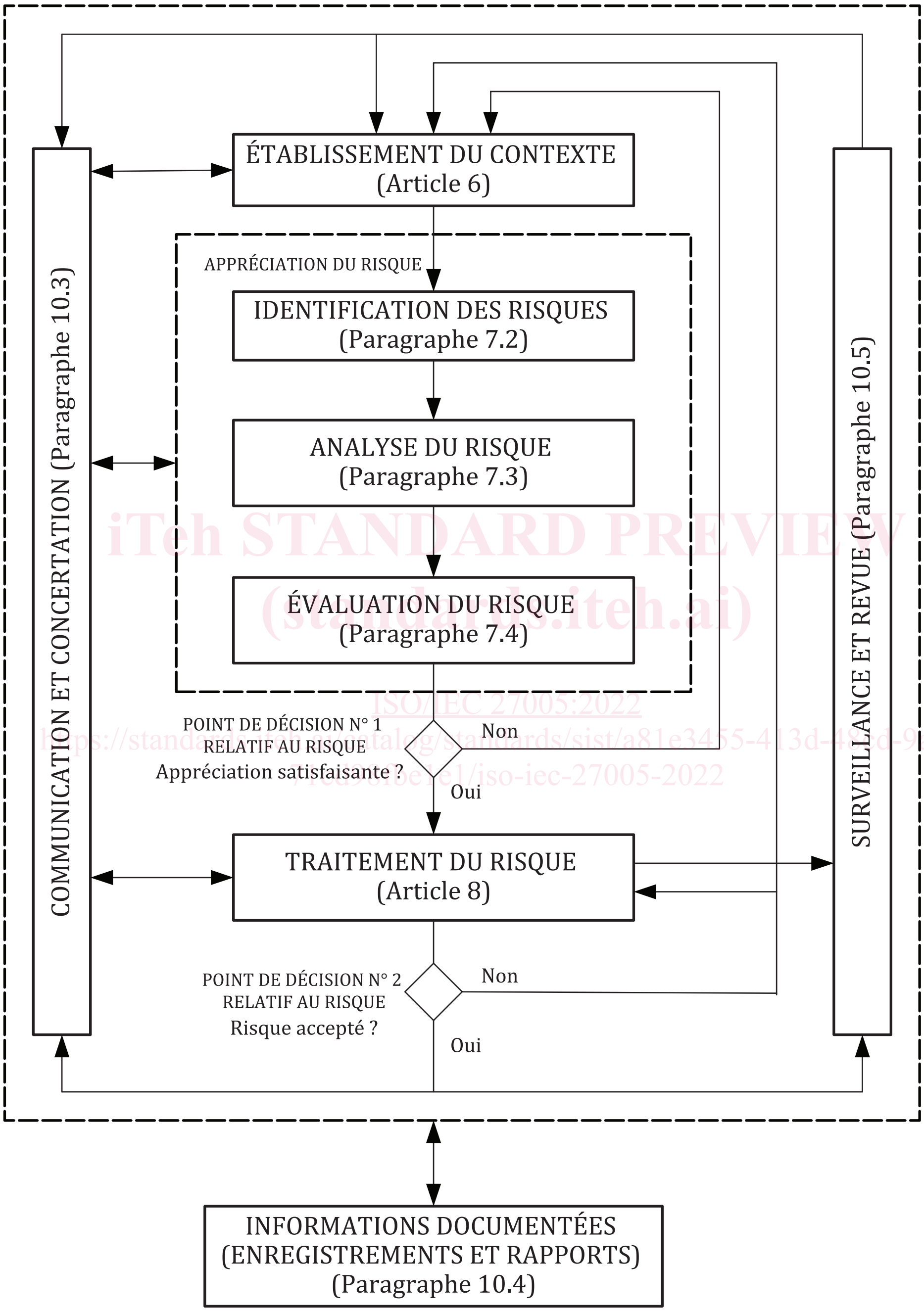

Figure 1 — Processus de gestion des risques liés à la sécurité de l'information

Comme l'illustre la Figure 1, le processus de gestion des risques liés à la sécurité de l'information peut être itératif pour les activités d'appréciation et/ou de traitement du risque. Une approche itérative de conduite de l'appréciation du risque permet d'approfondir et de préciser l'appréciation à chaque itération. Cette approche itérative assure un bon équilibre entre la minimisation du temps et des efforts investis dans l'identification des moyens de maîtrise et l'assurance que les risques sont correctement appréciés.

© ISO/IEC 2022 – Tous droits réservés

L'établissement du contexte implique de rassembler des informations sur les contextes externes et internes pour la gestion des risques ou l'appréciation du risque liées à la sécurité de l'information.

Si l'appréciation du risque donne suffisamment d'informations pour déterminer correctement les actions nécessaires pour ramener les risques à un niveau acceptable, la tâche est alors terminée et suivie par l'étape de traitement du risque. Si les informations sont insuffisantes, il convient d'effectuer une nouvelle itération de l'appréciation du risque. Cela peut impliquer un changement de contexte de l'appréciation du risque (par exemple, une révision du domaine d'application), l'implication d'une expertise dans le domaine concerné, ou d'autres moyens de collecter les informations nécessaires pour permettre de ramener le risque à un niveau acceptable (voir le «point de décision n°1 relatif au risque» à la Figure 1).

Le traitement du risque implique un processus itératif:

— formuler et choisir des options de traitement du risque;

— élaborer et mettre en œuvre le traitement du risque;

— apprécier l'efficacité de ce traitement;

— déterminer si le risque résiduel est acceptable;

— envisager un traitement complémentaire s'il n'est pas acceptable.

Il est possible que le traitement du risque ne génère pas immédiatement un niveau acceptable de risques résiduels. Dans ce cas, il est possible d'effectuer une nouvelle tentative pour identifier un traitement supplémentaire du risque, ou de procéder à une nouvelle itération complète ou partielle de l'appréciation du risque. Cela peut impliquer un changement de contexte de l'appréciation du risque (par exemple en cas de révision du domaine d'application) et l'implication d'une expertise dans le domaine concerné. La connaissance des menaces ou des vulnérabilités pertinentes peut conduire à de meilleures décisions concernant les activités de traitement du risque appropriées lors de l'itération suivante de l'appréciation du risque (voir le «point de décision n°2 relatif au risque» à la Figure 1).

L'établissement du contexte est décrit en détail à l'Article 6, les activités d'appréciation du risque à l'Article 7 et les activités de traitement du risque à l'Article 8.

D'autres activités nécessaires à la gestion des risques liés à la sécurité de l'information sont décrites à l'Article 10.

5.2 Cycles de gestion des risques liés à la sécurité de l'information

L'appréciation du risque et le traitement du risque doivent être mis à jour régulièrement et sur la base des changements effectués. Il convient que cela s'applique à l'appréciation du risque dans sa totalité, et les mises à jour peuvent être divisées en deux cycles de gestion du risque:

— le cycle stratégique, dans lequel les valeurs métier, les sources de risque et les menaces, les objectifs visés ou les conséquences sur les événements liés à la sécurité de l'information découlent des changements survenus dans le contexte général de l'organisme. Ces éléments peuvent servir d'éléments d'entrée pour une mise à jour globale de la ou des appréciations du risque et des traitements du risque. Ils peuvent également servir d'éléments d'entrée permettant d'identifier les nouveaux risques et de lancer des appréciations du risque entièrement nouvelles;

— le cycle opérationnel, dans lequel les éléments mentionnés ci-dessus servent d'informations d'entrée ou de critères modifiés qui auront une incidence sur une ou des appréciations du risque lors desquelles il convient que les scénarios soient revus et mis à jour. Il convient que la revue inclue la mise à jour du traitement du risque correspondant comme applicable.

Il convient que le cycle stratégique se déroule sur une période plus longue ou en cas de changements importants, tandis qu'il convient que le cycle opérationnel soit plus court en fonction des risques détaillés qui sont identifiés et appréciés, ainsi que du traitement associé du risque.

iTeh STANDARD PREVIEW
(standards.iteh.ai)