NORME INTERNATIONALE

ISO/IEC 27701

Première édition
2019-08

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Numéro de référence
ISO/IEC 27701:2019(F)

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

Sommaire

Page

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 document. 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'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.c).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité*.

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.

Introduction

0.1 Généralités

Toutes les organisations ou presque traitent des données à caractère personnel (DCP). En outre, la quantité et les types de DCP traitées sont en augmentation, de même que le nombre de situations où une organisation a besoin de collaborer avec d'autres organisations en ce qui concerne le traitement des DCP. La protection de la vie privée dans le contexte du traitement des DCP est une nécessité sociétale, ainsi que l'objet de législations et/ou de règlementations dédiées dans le monde entier.

Le système de management de la sécurité de l'information (SMSI) défini dans l'ISO/IEC 27001 est conçu pour permettre l'ajout d'exigences spécifiques à des secteurs, sans qu'il soit nécessaire de concevoir un nouveau système de management. Les normes de l'ISO relatives aux systèmes de management, y compris celles qui sont spécifiques à des secteurs, sont conçues pour pouvoir être mises en œuvre séparément ou sous la forme d'un système de management combiné.

Les exigences et les recommandations relatives à la protection des DCP varient selon le contexte de l'organisation, particulièrement lorsqu'une législation et/ou des règlementations nationales existent. La norme ISO/IEC 27001 exige la compréhension et la prise en compte de ce contexte. Le présent document inclut une mise en correspondance avec:

— les principes et le cadre de la protection de la vie privée définis dans l'ISO/IEC 29100;

— l'ISO/IEC 27018;

— l'ISO/IEC 29151; et

— le Règlement général sur la protection des données.

Toutefois, il peut être nécessaire d'interpréter ces derniers afin de tenir compte de la législation et/ou de la règlementation locale.

Le présent document peut être utilisé par les responsables de traitement de DCP (y compris ceux qui sont des responsables conjoints de traitement) et les sous-traitants de DCP (y compris ceux qui utilisent des sous-traitants de DCP sous-traitants et ceux qui traitent des DCP en tant que sous-traitants à des sous-traitants de DCP).

Une organisation se conformant aux exigences du présent document produira des preuves documentaires de la façon dont elle gère le traitement des DCP. Ces preuves peuvent être utilisées pour faciliter les accords avec les partenaires d'affaires là où les deux parties sont concernées par le traitement des DCP. Cela peut également faciliter les relations avec d'autres parties prenantes. L'utilisation du présent document conjointement avec l'ISO/IEC 27001 peut, si cela est souhaité, permettre une vérification indépendante de ces preuves.

Le présent document a initialement été élaboré en tant que norme ISO/IEC 27552.

0.2 Compatibilité avec les autres normes de systèmes de management

Le présent document applique le cadre élaboré par l'ISO afin d'améliorer l'harmonisation entre ses normes de systèmes de management.

Le présent document permet à une organisation d'aligner ou d'intégrer son PIMS aux exigences d'autres normes de systèmes de management.

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

1 Domaine d'application

Le présent document spécifie les exigences et fournit des recommandations pour la création, la mise en œuvre, le maintien et l'amélioration continue d'un système de management de la protection de la vie privée (PIMS) sous la forme d'une extension de l'ISO/IEC 27001 et l'ISO/IEC 27002 pour le management de la protection de la vie privée dans le contexte de l'organisation.

Le présent document spécifie les exigences liées au PIMS et fournit des recommandations destinées aux responsables de traitement de DCP et aux sous-traitants de DCP chargés de et responsables du traitement des DCP.

Le présent document s'applique aux organisations de tous types et de toutes tailles, y compris les entreprises publiques et privées, les entités gouvernementales et les organisations à but non lucratif, qui sont des responsables de traitement de DCP et/ou des sous-traitants de DCP qui traitent les DCP à l'aide d'un SMSI.

2 Références normatives

Les documents suivants cités dans le texte 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 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

ISO/IEC 29100, *Technologies de l'information — Techniques de sécurité — Cadre privé*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 27000 et l'ISO/IEC 29100 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 http://www.electropedia.org/

3.1
responsable conjoint de traitement
responsable de traitement de DCP qui détermine les finalités et les moyens du traitement des DCP conjointement avec un ou plusieurs autres responsables de traitement de DCP

3.2
système de management de la protection de la vie privée
PIMS
système de management de la sécurité de l'information qui gère la protection de la vie privée telle que potentiellement affectée par le traitement des DCP

4 Généralités

4.1 Structure du présent document

Il s'agit d'un document spécifique à un secteur lié à l'ISO/IEC 27001:2013 et à l'ISO/IEC 27002:2013.

Le présent document se focalise sur les exigences spécifiques au PIMS. La conformité au présent document se fonde sur l'adhésion à ces exigences et aux exigences de l'ISO/IEC 27001:2013. Le présent document étend les exigences de l'ISO/IEC 27001:2013 afin de prendre en compte la protection de la vie privée des personnes concernées telle que potentiellement affectée par le traitement des DCP, en plus de la sécurité de l'information. Pour une meilleure compréhension, des recommandations de mise en œuvre et des informations supplémentaires relatives aux exigences sont incluses.

L'Article 5 fournit des exigences spécifiques au PIMS et des informations supplémentaires relatives aux exigences en matière de sécurité de l'information contenues dans l'ISO/IEC 27001 appropriées pour une organisation agissant comme responsable de traitement de DCP ou comme sous-traitant de DCP.

NOTE 1 Dans un souci d'exhaustivité, l'Article 5 contient un paragraphe pour chacun des paragraphes de l'ISO/IEC 27001:2013 contenant des exigences, même dans les cas où il n'existe pas d'exigences spécifiques au PIMS ou d'informations supplémentaires.

L'Article 6 fournit des recommandations spécifiques au PIMS et des informations supplémentaires relatives aux mesures de sécurité de l'information contenues dans l'ISO/IEC 27002 et des recommandations spécifiques au PIMS pour une organisation agissant comme responsable de traitement de DCP ou comme sous-traitant de DCP.

NOTE 2 Dans un souci d'exhaustivité, l'Article 6 contient un paragraphe pour chacun des paragraphes de l'ISO/IEC 27002:2013 contenant des objectifs ou des mesures, même dans les cas où il n'existe pas de recommandations spécifiques au PIMS ou d'informations supplémentaires.

L'Article 7 fournit des recommandations supplémentaires de l'ISO/IEC 27002 pour les responsables de traitement de DCP, et l'Article 8 fournit des recommandations supplémentaires de l'ISO/IEC 27002 pour les sous-traitants de DCP.

L'Annexe A énumère les objectifs et mesures spécifiques au PIMS pour une organisation agissant comme responsable de traitement de DCP (qu'elle fasse appel à un sous-traitant de DCP ou non, et qu'elle agisse conjointement avec un autre responsable de traitement de DCP ou non).

L'Annexe B énumère les objectifs et mesures spécifiques au PIMS pour une organisation agissant comme sous-traitant de DCP (qu'elle sous-traite le traitement des DCP à un sous-traitant de DCP distinct ou non, et y compris ceux qui traitent les DCP comme sous-traitants de sous-traitants de DCP).

L'Annexe C contient un tableau de correspondance avec l'ISO/IEC 29100.

L'Annexe D contient un tableau de correspondance des mesures du présent document avec le Règlement général sur la protection des données.

L'Annexe E contient un tableau de correspondance avec l'ISO/IEC 27018 et l'ISO/IEC 29151.

L'Annexe F explique comment l'ISO/IEC 27001 et l'ISO/IEC 27002 sont étendues à la protection de la vie privée lors du traitement de DCP.

4.2 Application des exigences de l'ISO/IEC 27001:2013

Le Tableau 1 indique l'emplacement des exigences spécifiques au PIMS contenues dans le présent document par rapport à l'ISO/IEC 27001.

Tableau 1 — Emplacement des exigences spécifiques au PIMS et des informations supplémentaires pour la mise en œuvre des mesures de l'ISO/IEC 27001:2013

Article de l'ISO/IEC 27001:2013	Titre	Paragraphe du présent document	Remarques
4	Contexte de l'organisation	5.2	Exigences supplémentaires
5	Leadership	5.3	Aucune exigence spécifique au PIMS
6	Planification	5.4	Exigences supplémentaires
7	Support	5.5	Aucune exigence spécifique au PIMS
8	Fonctionnement	5.6	Aucune exigence spécifique au PIMS
9	Évaluation des performances	5.7	Aucune exigence spécifique au PIMS
10	Amélioration	5.8	Aucune exigence spécifique au PIMS

NOTE L'interprétation étendue de «sécurité de l'information» conformément au paragraphe 5.1 s'applique toujours, même en l'absence d'exigences spécifiques au PIMS.

4.3 Application des lignes directrices de l'ISO/IEC 27002:2013

Le Tableau 2 indique l'emplacement des recommandations spécifiques au PIMS contenues dans le présent document par rapport à l'ISO/IEC 27002.

Tableau 2 — Emplacement des recommandations spécifiques au PIMS et des informations supplémentaires pour la mise en œuvre des mesures de l'ISO/IEC 27002:2013

Article de l'ISO/IEC 27002:2013	Titre	Paragraphe du présent document	Remarques
5	Politiques de sécurité de l'information	6.2	Recommandations supplémentaires
6	Organisation de la sécurité de l'information	6.3	Recommandations supplémentaires
7	La sécurité des ressources humaines	6.4	Recommandations supplémentaires
8	Gestion des actifs	6.5	Recommandations supplémentaires
9	Contrôle d'accès	6.6	Recommandations supplémentaires
10	Cryptographie	6.7	Recommandations supplémentaires
11	Sécurité physique et environnementale	6.8	Recommandations supplémentaires
12	Sécurité liée à l'exploitation	6.9	Recommandations supplémentaires
13	Sécurité des communications	6.10	Recommandations supplémentaires
14	Acquisition, développement et maintenance des systèmes d'information	6.11	Recommandations supplémentaires
15	Relations avec les fournisseurs	6.12	Recommandations supplémentaires
16	Gestion des incidents liés à la sécurité de l'information	6.13	Recommandations supplémentaires

Tableau 2 *(suite)*

Article de l'ISO/IEC 27002:2013	Titre	Paragraphe du présent document	Remarques
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	6.14	Aucune recommandation spécifique au PIMS
18	Conformité	6.15	Recommandations supplémentaires

NOTE L'interprétation étendue de «sécurité de l'information» conformément au paragraphe 6.1 s'applique toujours, même en l'absence de recommandations spécifiques au PIMS.

4.4 Client

Selon le rôle de l'organisation (voir 5.2.1), le terme «client» peut être compris comme signifiant:

a) une organisation qui a conclu un contrat avec un responsable de traitement de DCP (par exemple: le client du responsable de traitement de DCP);

NOTE 1 Cela peut être le cas d'une organisation qui est un responsable conjoint de traitement.

NOTE 2 Une personne physique ayant, avec une organisation, une relation de consommateur à entreprise est qualifiée de «personne concernée» dans le présent document.

b) un responsable de traitement de DCP qui a conclu un contrat avec un sous-traitant de DCP (par exemple: le client du sous-traitant de DCP); ou

c) un sous-traitant de DCP qui a conclu un contrat avec un sous-traitant pour le traitement de DCP (par exemple: le client du sous-traitant du sous-traitant).

NOTE 3 Lorsque le terme «client» est mentionné dans l'Article 6, les dispositions afférentes peuvent être applicables dans les contextes a), b) ou c).

NOTE 4 Lorsque le terme «client» est mentionné dans l'Article 7 et l'Annexe A, les dispositions afférentes sont applicables dans le contexte a).

NOTE 5 Lorsque le terme «client» est mentionné dans l'Article 8 et l'Annexe B, les dispositions afférentes peuvent être applicables dans les contextes b) et/ou c).

5 Exigences spécifiques au PIMS liées à l'ISO/IEC 27001

5.1 Généralités

Les exigences de l'ISO/IEC 27001:2013 mentionnant la «sécurité de l'information» doivent être étendues à la protection de la vie privée telle que potentiellement affectée par le traitement des DCP.

NOTE Dans la pratique, lorsque le terme «sécurité de l'information» est utilisé dans l'ISO/IEC 27001:2013, «sécurité de l'information et protection de la vie privée» s'applique à la place (voir l'Annexe F).

5.2 Contexte de l'organisation

5.2.1 Compréhension de l'organisation et de son contexte

Exigence supplémentaire par rapport au paragraphe 4.1 de l'ISO/IEC 27001:2013:

L'organisation doit déterminer son rôle comme responsable de traitement de DCP (y compris comme responsable conjoint de traitement) et/ou comme sous-traitant de DCP.

L'organisation doit déterminer les facteurs externes et internes pertinents pour son contexte, et qui influent sur sa capacité à atteindre le ou les résultat(s) attendu(s) de son PIMS. Par exemple, ceux-ci peuvent comprendre:

— législation applicable en matière de protection de la vie privée;

— réglementations applicables;

— décisions judiciaires applicables;

— contexte, gouvernance, politiques et procédures organisationnels applicables;

— décisions administratives applicables;

— exigences contractuelles applicables.

Lorsque l'organisation agit dans les deux rôles (par exemple: comme responsable de traitement de DCP et comme sous-traitant de DCP), les différents rôles doivent être déterminés, chacun d'entre eux faisant l'objet d'une série de mesures distinctes.

NOTE Le rôle de l'organisation peut être différent pour chaque instance du traitement des DCP, étant donné qu'il dépend de qui détermine les finalités et les moyens du traitement.

5.2.2 Compréhension des besoins et des attentes des parties intéressées

Exigence supplémentaire par rapport au paragraphe 4.2 de l'ISO/IEC 27001:2013:

L'organisation doit inclure parmi ses parties intéressées (voir l'ISO/IEC 27001:2013, 4.2), les parties ayant des intérêts ou des responsabilités associés au traitement des DCP, y compris les personnes concernées.

NOTE 1 Les autres parties intéressées peuvent inclure les clients (voir 4.4), les autorités de contrôle, d'autres responsables de traitement de DCP, les sous-traitants de DCP et leurs sous-traitants.

NOTE 2 Les exigences pertinentes pour le traitement des DCP peuvent être déterminées par les exigences légales et réglementaires, par les obligations contractuelles et les objectifs que l'organisation s'impose elle-même. Les principes de protection de la vie privée énoncés dans l'ISO/IEC 29100 fournissent des recommandations concernant le traitement des DCP.

NOTE 3 En guise d'élément démontrant la conformité aux obligations de l'organisation, certaines parties intéressées peuvent attendre de l'organisation qu'elle se conforme à des normes spécifiques, telles que le système de management spécifié dans le présent document, et/ou à tout ensemble pertinent de spécifications. Ces parties peuvent demander que la conformité à ces normes fasse l'objet d'un audit indépendant.

5.2.3 Détermination du domaine d'application du système de management de la sécurité de l'information

Exigence supplémentaire par rapport au paragraphe 4.3 de l'ISO/IEC 27001:2013:

Lors de la détermination du périmètre du PIMS, l'organisation doit inclure le traitement des DCP.

NOTE La détermination du périmètre du PIMS peut nécessiter de réviser le périmètre du système de management de la sécurité de l'information, en raison de l'interprétation étendue de «sécurité de l'information» conformément au paragraphe 5.1.

5.2.4 Système de management de la sécurité de l'information

Exigence supplémentaire par rapport au paragraphe 4.4 de l'ISO/IEC 27001:2013:

L'organisation doit créer, mettre en œuvre, tenir à jour et améliorer continuellement un PIMS conformément aux exigences des Articles 4 à 10 de l'ISO/IEC 27001:2013, étendus par les exigences de l'Article 5.

5.3 Leadership

5.3.1 Leadership et engagement

Les exigences énoncées au paragraphe 5.1 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.3.2 Politique

Les exigences énoncées au paragraphe 5.2 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.3.3 Rôles, responsabilités et autorités au sein de l'organisation

Les exigences énoncées au paragraphe 5.3 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.4 Planification

5.4.1 Actions face aux risques et opportunités

5.4.1.1 Généralités

Les exigences énoncées au paragraphe 6.1.1 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.4.1.2 Appréciation des risques de sécurité de l'information

Les exigences énoncées au paragraphe 6.1.2 de l'ISO/IEC 27001:2013 s'appliquent, avec les affinements suivants:

L'ISO/IEC 27001:2013, 6.1.2 c) 1) est affinée comme suit:

L'organisation doit appliquer le processus d'appréciation des risques de sécurité de l'information pour identifier les risques liés à la perte de confidentialité, d'intégrité et de disponibilité entrant dans le périmètre du PIMS.

L'organisation doit appliquer un processus d'appréciation des risques sur la vie privée pour identifier les risques liés au traitement des DCP, entrant dans le périmètre du PIMS.

L'organisation doit s'assurer tout au long des processus d'appréciation des risques que la relation entre la sécurité de l'information et la protection des DCP est gérée de façon appropriée.

NOTE L'organisation peut appliquer un processus d'appréciation des risques de sécurité de l'information et de risques sur la vie privée intégré ou deux processus distincts pour la sécurité de l'information et les risques associés au traitement des DCP.

L'ISO/IEC 27001:2013, 6.1.2 d) 1) est affinée comme suit:

L'organisation doit évaluer les conséquences potentielles pour l'organisation et pour les personnes concernées si les risques identifiés dans l'ISO/IEC 27001:2013, 6.1.2 c) telle qu'affinée ci-dessus, se concrétisaient.

5.4.1.3 Traitement des risques de sécurité de l'information

Les exigences énoncées au paragraphe 6.1.3 de l'ISO/IEC 27001:2013 s'appliquent, avec les ajouts suivants:

L'ISO/IEC 27001:2013, 6.1.3 c) est affinée comme suit:

Les mesures déterminées dans l'ISO/IEC 27001:2013 6.1.3 b) doivent être comparées aux mesures de l'Annexe A et/ou de l'Annexe B et de l'ISO/IEC 27001:2013, Annexe A afin de vérifier qu'aucune mesure nécessaire n'a été omise.

Lors de l'évaluation de l'applicabilité des objectifs et des mesures de l'Annexe A de l'ISO/IEC 27001:2013 pour le traitement des risques, les objectifs et les mesures doivent être envisagés dans le contexte tant des risques pour la sécurité de l'information que des risques liés au traitement des DCP, y compris les risques pour les personnes concernées.

L'ISO/IEC 27001:2013, 6.1.3 d) est affinée comme suit:

Produire une Déclaration d'applicabilité contenant:

— les mesures nécessaires [voir l'ISO/IEC 27001:2013, 6.1.3 b) et c)];

— la justification de leur insertion;

— si les mesures nécessaires sont mises en œuvre ou non; et

— la justification de l'exclusion de toute mesure de l'Annexe A et/ou de l'Annexe B et de l'ISO/IEC 27001:2013, Annexe A conformément à la détermination, par l'organisation, de son rôle (voir 5.2.1).

Il n'est pas nécessaire d'inclure tous les objectifs et toutes les mesures énumérés dans les annexes dans la mise en œuvre d'un PIMS. La justification de l'exclusion peut inclure les cas où les mesures ne sont pas jugées nécessaires par l'appréciation des risques, et ceux où elles ne sont pas requises par (ou sont soumises à des exceptions en vertu de) la législation et/ou la règlementation, y compris celles applicables à la personne concernée.

5.4.2 Objectifs de sécurité de l'information et plans pour les atteindre

Les exigences énoncées au paragraphe 6.2 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.5 Support

5.5.1 Ressources

Les exigences énoncées au paragraphe 7.1 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.5.2 Compétence

Les exigences énoncées au paragraphe 7.2 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.5.3 Sensibilisation

Les exigences énoncées au paragraphe 7.3 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.

5.5.4 Communication

Les exigences énoncées au paragraphe 7.4 de l'ISO/IEC 27001:2013, ainsi que l'interprétation spécifiée en 5.1, s'appliquent.