ISO/IEC JTC 1/SC 27

Date~~-~~: 2022-~~02~~10

~~**Version corrigée : 2022-03**~~

ISO IEC 27002:2022 (F)

ISO/IEC JTC 1/SC 27

Secrétariat~~-~~: DIN

Sécurité de l'information, cybersécurité et protection de la vie privée — Moyens de maîtrise de l'information

Information security, cybersecurity and privacy protection — Information security controls

~~ICS : 35.030~~

Type du document: Norme internationale
Sous-type du document:
Stade du document: (60) Publication
Langue du document: F

Type du document: Norme internationale
Sous-type du document:
Stade du document: (60) Publication
Langue du document: F

ISO copyright office

CP 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

Avant-propos

L'ISO (Organisation internationale de normalisation) et ~~l'IEC~~l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de ~~l'IEC~~l'IEC participent au développement de Normes ~~Internationales~~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~~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~~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~~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~~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~~www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir ~~patents.iec.ch~~https://patents.iec.ch).

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'Organisation~~l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir ~~le lien suivant : www.iso.org/iso/fr/avant-propos~~www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

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 troisième édition annule et remplace la deuxième édition (ISO/IEC 27002:2013~~)~~), qui a fait ~~l'objet d'une~~l'objet d'une révision technique. Elle ~~contient~~incorpore également les ~~rectificatifs~~Rectificatifs techniques ISO/IEC 27002:2013/Cor. 1:2014 et ISO/IEC 27002:2013/Cor. 2:2015.

Les principales modifications sont les suivantes :

— le titre a été modifié ;

— la structure du document a été modifiée, présentant les moyens de maîtrise avec une taxonomie simple et des attributs associés ;

— certains moyens de maîtrise ont été fusionnés, d'autres ont été supprimés, et plusieurs nouveaux moyens de maîtrise ont été ajoutés. La correspondance complète se trouve à l'Annexe B.

La présente version ~~corrigée~~française de l'ISO/IEC 27002:2022 ~~comprend les corrections suivantes :~~

~~— les hyperliens qui ne fonctionnaient pas dans l'ensemble du document ont été restaurés ;~~

~~— dans~~correspond à la version anglaise publiée le ~~tableau introductif en 5.22~~2022-02 et ~~dans~~corrigé le ~~Tableau A.1 (ligne 5.22), « #Assurance_de_sécurité_de_l'information » a été déplacé de la colonne intitulée « Domaines de sécurité » vers la colonne intitulée « Capacités opérationnelles ».~~2022-03.

Il convient que ~~l'utilisateur~~l'utilisateur adresse tout retour ~~d'information~~d'information ou toute question concernant le présent document à ~~l'organisme~~l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve ~~aux adresses~~à l'adresse ~~www.iso.org/fr/members.html~~www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

0.1 Historique et contexte

Le présent document a été conçu à l'intention des organisations de tous types et de toutes dimensions. Il est à utiliser comme document de référence pour déterminer et mettre en œuvre des moyens de maîtrise pour le traitement des risques liés à la sécurité de l'information dans un système de management de la sécurité de l'information (SMSI) basé sur l'ISO/IEC 27001. Il peut également être utilisé comme guide de bonnes pratiques pour les organisations qui déterminent et mettent en œuvre les moyens de maîtrise de l'information communément admis. De plus, le présent document a pour objet d'être utilisé lors de l'élaboration des lignes directrices de gestion de la sécurité de l'information spécifiques aux organisations et aux industries, en tenant compte de leur(s) environnement(s) spécifique(s) de risques liés à la sécurité de l'information. Des moyens de maîtrise organisationnels ou spécifiques à l'environnement autres que ceux qui figurent dans le présent document peuvent, si nécessaire, être déterminés par le biais de l'appréciation du risque.

Des organisations de tous types et de toutes dimensions (y compris du secteur public et du secteur privé, à but lucratif ou non lucratif) créent, collectent, traitent, stockent, transmettent et éliminent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, les conversations et les présentations).

La valeur de l'information va au-delà des mots, chiffres et images écrits : la connaissance, les concepts, les idées et les marques sont des exemples de formes intangibles d'information. Dans un monde interconnecté, les informations et autres actifs associés méritent ou exigent une protection contre différentes sources de risques, aussi bien naturelles, qu'accidentelles ou délibérées.

La sécurité de l'information est réalisée par la mise en œuvre d'un ensemble de moyens de maîtrise appropriés, notamment des politiques, des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles. Pour atteindre ses objectifs métier et de sécurité, il convient que l'organisation définisse, mette en œuvre, surveille, révise et améliore ces moyens de maîtrise au besoin. Un système de management de la sécurité de l'information (SMSI) tel que celui spécifié dans l'ISO/IEC 27001 appréhende les risques liés à la sécurité de l'information de l'organisation dans une vision globale et coordonnée, afin de déterminer et mettre en œuvre un ensemble complet de moyens de maîtrise de l'information dans le cadre global d'un système de management cohérent.

De nombreux systèmes d'information, y compris leur management et leurs opérations, n'ont pas été conçus sécurisés au sens d'un système de management de la sécurité de l'information tel que spécifié dans l'ISO/IEC 27001 et le présent document. Le niveau de sécurité qui peut être atteint seulement par des mesures techniques est limité, et il convient de le renforcer par des processus organisationnels et activités de management appropriés. L'identification des moyens de maîtrise qu'il convient de mettre en place nécessite une planification minutieuse et une attention aux détails lors de la réalisation du traitement du risque.

Un système de management de la sécurité de l'information réussi requiert l'adhésion de tout le personnel de l'organisation. Il peut également nécessiter la participation d'autres parties intéressées, telles que des actionnaires ou des fournisseurs. Des conseils d'experts en la matière peuvent aussi s'avérer nécessaires.

Un système de management de la sécurité de l'information approprié, adéquat et efficace procure la garantie aux dirigeants de l'organisation et autres parties intéressées que leurs informations et autres actifs associés sont suffisamment sécurisés et protégés contre les menaces et dommages, ce qui permet à l'organisation d'atteindre les objectifs métier visés.

0.2 Exigences de sécurité de l'information

Il est essentiel qu'une organisation détermine ses exigences de sécurité de l'information. Il existe trois principales sources des exigences de sécurité de l'information :

a) l'appréciation du risque de l'organisation, prenant en compte l'ensemble de sa stratégie et objectifs métier. Cela peut être facilité ou appuyé par une appréciation du risque lié à la sécurité de l'information. Il convient que cela aboutisse à la détermination les moyens de maîtrise nécessaires assurant que les risques résiduels pour l'organisation correspondent à ses critères d'acceptation des risques ;

b) les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses parties intéressées (partenaires commerciaux, fournisseurs de services, etc.) doivent se conformer ainsi que leur environnement socioculturel ;

c) l'ensemble des principes, d'objectifs et d'exigences métier pour toutes les étapes du cycle de vie de l'information que l'organisation a élaboré pour appuyer son fonctionnement.

0.3 Moyens de maîtrise

Un moyen de maîtrise est défini comme une mesure qui modifie ou maintient un risque. Certains des moyens de maîtrise dans le présent document sont des moyens qui modifient les risques, tandis que d'autres maintiennent les risques. Une politique de sécurité de l'information, par exemple, permet seulement de maintenir les risques, tandis que la conformité à la politique de sécurité de l'information peut modifier les risques. De plus, certains moyens de maîtrise décrivent la même mesure générique dans différents contextes de risques. Le présent document propose une combinaison générique de moyens de maîtrise de l'information organisationnels, liés aux personnes, physiques et technologiques, issus des bonnes pratiques reconnues au niveau international.

0.4 Détermination des moyens de maîtrise

La détermination des moyens de maîtrise dépend des décisions de l'organisation suite à une appréciation du risque, avec un périmètre clairement défini. Il convient de baser les décisions relatives aux risques identifiés sur les critères d'acceptation des risques, les options de traitement des risques et l'approche de gestion des risques appliqués par l'organisation. Il convient également que la détermination des moyens de maîtrise tienne compte de toutes les législations et réglementations nationales et internationales pertinentes. La détermination des moyens de maîtrise dépend aussi de la manière dont les moyens de maîtrise interagissent les uns avec les autres pour assurer une défense en profondeur.

L'organisation peut concevoir des moyens de maîtrise au besoin, ou bien les identifier à partir de n'importe quelle source. Lors de la spécification de ces moyens de maîtrise, il convient que l'organisation tienne compte des ressources et investissements nécessaires pour mettre en œuvre et opérer un moyen de maîtrise par rapport à la valeur métier réalisée. Voir l'ISO/IEC TR 27016 pour les recommandations sur les décisions concernant les investissements dans un SMSI et les conséquences économiques de ces décisions dans le contexte d'exigences concurrentes en matière de ressources.

Il convient qu'il y ait un équilibre entre les ressources déployées pour mettre en œuvre les moyens de maîtrise et l'impact métier possible résultant des incidents de sécurité en l'absence de ces moyens de maîtrise. Il convient que les résultats de l'appréciation du risque aide à guider et à déterminer les actions de gestion appropriées, les priorités pour gérer les risques de sécurité de l'information, et pour mettre en œuvre les moyens de maîtrise identifiés comme nécessaires pour protéger contre ces risques.

Certains moyens de maîtrise dans le présent document peuvent être considérés comme des principes de base pour la gestion de la sécurité de l'information et ils sont applicables à la plupart des organisations. Plus d'informations sur la détermination des moyens de maîtrise et autres options de traitement du risque peuvent être trouvées dans l'ISO/IEC 27005.

0.5 Élaboration de lignes directrices spécifiques à une organisation

Le présent document peut être considéré comme point de départ pour l'élaboration de lignes directrices spécifiques à une organisation. Tous les moyens de maîtrise et lignes directrices du présent document peuvent ne pas être applicables à toutes les organisations. D'autres moyens de maîtrise et lignes directrices ne figurant pas dans le présent document peuvent être nécessaires pour traiter les besoins spécifiques de l'organisation et les risques identifiés. Lors de la rédaction de documents contenant des lignes directrices ou des moyens de maîtrise supplémentaires, il peut être utile d'ajouter des références croisées aux articles du présent document en vue d'une consultation ultérieure.

0.6 Considérations relatives au cycle de vie

L'information a un cycle de vie, depuis sa création jusqu'à son élimination. La valeur de l'information et les risques associés peuvent varier au cours de ce cycle de vie (par exemple, une divulgation non autorisée ou le vol des comptes financiers d'une entreprise n'a pas d'impact significatif après la publication de ces informations, mais l'intégrité demeure critique). Par conséquent, l'importance de la sécurité de l'information subsiste à tous les stades.

Les systèmes d'information et autres actifs pertinents pour la sécurité de l'information ont des cycles de vie durant lesquels ils sont pensés, spécifiés, conçus, développés, testés, mis en œuvre, utilisés, maintenus et finalement retirés du service et mis au rebut. Il convient que la sécurité de l'information soit considérée à chaque étape. Les projets de développement de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion d'améliorer les moyens de maîtrise tout en prenant en compte les risques de l'organisation et les leçons tirées des incidents.

0.7 Normes internationales associées

Alors que le présent document propose des recommandations portant sur un vaste éventail de moyens de maîtrise qui sont communément utilisés dans plusieurs organisations différentes, d'autres documents de la famille ISO/IEC 27000 proposent des conseils complémentaires ou des exigences relatifs à d'autres aspects du processus global de gestion de la sécurité de l'information.

Se reporter à l'ISO/IEC 27000 pour une introduction générale à la fois aux SMSI et à la famille de documents. L'ISO/IEC 27000 fournit un glossaire, définissant la plupart des termes utilisés dans la famille des documents ISO/IEC 27000, et décrit le périmètre et les objectifs de chaque membre de la famille.

Il existe des normes sectorielles qui comportent des moyens de maîtrise supplémentaires destinés à traiter des domaines spécifiques (par exemple, l'ISO/IEC 27017 pour les services en nuage, l'ISO/IEC 27701 pour la protection de la vie privée, l'ISO/IEC 27019 pour l'énergie, l'ISO/IEC 27011 pour les organismes de télécommunications et l'ISO 27799 pour la santé). Ces normes figurent dans la Bibliographie et certaines d'entre elles sont référencées dans les recommandations et autres informations des Articles 5 à 8.