NORME INTERNATIONALE

ISO/IEC 27002

Redline version
compare la Deuxième édition
à la Troisième édition

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

Numéro de référence
ISO/IEC27002:redline:2023(F)

IMPORTANT — PLEASE NOTE

This is a provisional 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

All changes in this document have yet to reach concensus by vote and as such should only be used internally for review purposes.

DISCLAIMER

This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions and deletions are displayed in red, with deletions being struck through.

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

Avant-propos

L'ISO (Organisation internationale de normalisation) et ~~la CEI~~l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de ~~la CEI~~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 ~~la CEI~~l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et ~~la CEI~~l'IEC, participent également aux travaux. ~~Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.~~

Les ~~Normes internationales sont rédigées~~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/~~CEI~~IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

~~La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.~~

L'attention est ~~appelée~~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 ~~ne saurait être tenue pour responsable~~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).

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.

~~L'ISO/CEI 27002~~Le présent document a été ~~élaborée~~élaboré par le comité technique mixte ISO/~~CEI TC~~IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, ~~*Techniques de sécurité des technologies de l'information*~~*Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette ~~deuxième~~troisième édition annule et remplace la ~~première~~deuxième édition (ISO/~~CEI~~IEC 27002:~~2005~~2013), qui a fait ~~l'objet d'une révision technique~~l'objet d'une révision technique. Elle incorpore également les Rectificatifs techniques ISO/IEC 27002:2013/Cor. 1:2014 et ~~structurelle~~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 française de l'ISO/IEC 27002:2022 correspond à la version anglaise publiée le 2022-02 et corrigé le 2022-03.

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/members.html et www.iec.ch/national-committees.

0 Introduction

0.1 Historique et contexte

La présente Norme internationale a pour objet de servir d'outil de référence permettant aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'unLe 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) selonbasé sur l'ISO/CEIIEC 27001[10] ou de guide. Il peut également être utilisé comme guide de bonnes pratiques pour les organisations mettant en œuvre des mesures de sécurité de l'information largement reconnues. La présente norme a également pour objet d'élaborerqui 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 managementgestion de la sécurité de l'information spécifiques aux organisations et aux entreprisesindustries, en tenant compte de leur(s) environnement(s) particulierspécifique(s) de risques deliés 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 (incluant ley compris du secteur public et ledu secteur privé, à but lucratif ou non lucratif) créent, collectent, traitent, stockent et transmettent, transmettent et éliminent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, au cours deles conversations et deles présentations).

La valeur de l'information dépasse les mots, les chiffres et les imagesva au-delà des mots, chiffres et images écrits: la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles intangibles d'information. Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rattachent, ainsi que le personnel impliqué dans son traitement, ses manipulations et sa protection, sont des actifs précieux pour l'activité d'une organisation, au même titre que d'autres actifs d'entreprise importants, et, par conséquent, ils méritent ou nécessitent d'être protégés contre les divers risques encourusles informations et autres actifs associés méritent ou exigent une protection contre différentes sources de risques, aussi bien naturelles, qu'accidentelles ou délibérées.

Les actifs sont exposés à des menaces tant accidentelles que délibérées, alors que les processus, les systèmes, les réseaux et les personnes qui s'y rattachent présentent des vulnérabilités qui leur sont propres. Des changements apportés aux processus et aux systèmes de l'organisation ou d'autres changements externes (comme l'application de nouvelles lois et réglementations) peuvent engendrer de nouveaux risques pour la sécurité de l'information. Par conséquent, étant donné que les menaces disposent d'une multitude de possibilités d'exploitation des vulnérabilités pour nuire à l'organisation, les risques de sécurité de l'information sont omniprésents. Une sécurité efficace de l'information réduit ces risques en protégeant l'organisation contre les menaces et les vulnérabilités, ce qui réduit les conséquences sur ses actifs.

La sécurité de l'information est assuréel'information est réalisée par la mise en œuvre de mesures adaptées, qui regroupent desd'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. Ces mesures doivent être spécifiées, misesPour atteindre ses objectifs métier et de sécurité, il convient que l'organisation définisse, mette en œuvre, suivies, réexaminées et améliorées aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'une organisationsurveille, 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/CEIIEC 27001[10] appréhende les risques deliés à la sécurité de l'information de l'organisation dans une vision globale et coordonnée, de manière àafin de déterminer et mettre en œuvre un ensemble complet de mesures liées à la sécurité demoyens de maîtrise de l'information dans le cadre généralglobal d'un système de management cohérent.

~~Nombreux sont les systèmes d'information qui n'ont pas été conçus dans un souci de sécurité au sens de l'ISO/CEI 27001[10] et de la présente norme. La sécurité qui peut être mise en œuvre par des moyens techniques est limitée et il convient de la soutenir à l'aide de moyens de management et de procédures adaptés. L'identification des mesures qu'il convient de mettre en place nécessite de procéder à une planification minutieuse et de prêter attention aux détails. Un système de management de la sécurité de l'information efficace requiert l'adhésion de tous les salariés de l'organisation. Il peut également nécessiter la participation des actionnaires, des fournisseurs ou d'autres tiers. De même, l'avis de spécialistes tiers peut se révéler nécessaire.~~

~~De manière plus générale, une sécurité de l'information efficace garantit également à la direction et aux parties tiers que les actifs de l'organisation sont, dans des limites raisonnables, sécurisés et à l'abri des préjudices, et contribuent de ce fait au succès de l'organisation.~~

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 ~~liées à la sécurité de l'information~~de sécurité de l'information

~~Une organisation doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales.~~

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 propre à l'organisation, prenant en compte sa stratégie et ses objectifs généraux. L'appréciation du risque permet d'identifier les menaces pesant sur les actifs, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel;~~

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~~l'organisation et ses parties intéressées (partenaires commerciaux, ~~contractants et prestataires de service, doivent répondre~~fournisseurs de services, etc.) doivent se conformer ainsi que leur environnement socioculturel;

c) l'ensemble ~~de~~des principes, d'objectifs et d'exigences métier ~~en matière de manipulation, de traitement, de stockage, de communication et d'archivage de~~pour toutes les étapes du cycle de vie de l'information que l'organisation ~~s'est constitué pour mener à bien ses activités~~a élaboré pour appuyer son fonctionnement.

~~Il est nécessaire de confronter les ressources mobilisées par la mise en œuvre des mesures avec les dommages susceptibles de résulter de défaillances de la sécurité en l'absence de ces mesures. Les~~

~~résultats d'une appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de gestion des risques liés à la sécurité de l'information, ainsi que de mettre en œuvre les mesures identifiées destinées à contrer ces risques.~~

~~La norme ISO/CEI 27005[11] fournit des lignes directrices de gestion du risque lié à la sécurité de l'information, y compris des conseils sur l'appréciation du risque, le traitement du risque, l'acceptation du risque, la communication relative au risque, la surveillance du risque et la revue du risque.~~

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.

~~0.3 Sélection des mesures~~0.4 Détermination des moyens de maîtrise

~~Selon les cas, il est possible de sélectionner les mesures dans la présente norme ou dans d'autres guides, ou encore de spécifier de nouvelles mesures en vue de satisfaire des besoins spécifiques.~~

La ~~sélection des mesures~~détermination des moyens de maîtrise dépend des décisions ~~prises par l'organisation en fonction de ses critères d'acceptation~~de l'organisation suite à une appréciation du risque, ~~de ses~~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 ~~du risque et de son approche de la gestion générale du risque~~des risques et l'approche de gestion des risques appliqués par l'organisation. Il convient également ~~de prendre en considération les lois et règlements nationaux et internationaux concernés. La sélection des mesures de sécurité dépend 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 ~~mesures interagissent~~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.

~~Certaines mesures décrites dans la présente norme peuvent être considérées~~Certains moyens de maîtrise dans le présent document peuvent être considérés comme des principes ~~directeurs pour le management~~de base pour la gestion de la sécurité de ~~l'information et être appliquées~~l'information et ils sont applicables à la plupart des organisations. ~~Les mesures et des lignes directrices de mise en œuvre sont détaillées ci-dessous. De plus amples informations sur la sélection des mesures et d'autres~~Plus d'informations sur la détermination des moyens de maîtrise et autres options de traitement du risque ~~figurent~~peuvent être trouvées dans l'ISO/~~CEI~~IEC 27005.[11]

~~0.4 Mise au point~~0.5 Élaboration de lignes directrices ~~propres à l'organisation~~spécifiques à une organisation

La présente Norme internationale peut servir de base pour la mise au pointLe présent document peut être considéré comme point de départ pour l'élaboration de lignes directrices spécifiques à une organisation. Une partie des mesuresTous les moyens de maîtrise et lignes directrices de ce code de bonnes pratiques peutdu présent document peuvent ne pas être applicable. Par ailleurs, des mesures et desapplicables à toutes les organisations. D'autres moyens de maîtrise et lignes directrices ne figurant pas dans la présente normele 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 mesuresmoyens de maîtrise supplémentaires, il peut être utile d'intégrerd'ajouter des références croisées aux articles de la présente norme, le cas échéant, afin de faciliter la vérification de la conformité par les auditeurs et les partenaires commerciauxdu présent document en vue d'une consultation ultérieure.

0.5 Examen du0.6 Considérations relatives au cycle de vie

L'information est soumise àa un cycle de vie naturel, depuis sa création et son origine en passant par son stockage, son traitement, son utilisation, sa transmission, jusqu'à sa destruction finale ou son obsolescencejusqu'à son élimination. La valeur des actifsde l'information et les risques qui y sont liésassociés peuvent varier au cours de la duréece cycle de vie de ces actifs (par exemple, une divulgation non autorisée ou le vol des comptes financiers d'une entreprise revêt une importance bien moins grande après leur publication officielle), mais dans une certaine mesure l'importancen'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'informationl'information subsiste à tous les stades.

Les systèmes d'information sont soumis àet autres actifs pertinents pour la sécurité de l'information ont des cycles de vie durant lesquels ils sont pensés, caractérisésspécifiés, conçus, mis au pointdéveloppés, testés, mis en œuvre, utilisés, entretenusmaintenus et finalement retirés du service et mis au rebut. Il convient que la sécurité de l'information soit prise en compte à tous les stades. La mise au pointconsidérée à chaque étape. Les projets de développement de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion aux organisations de mettre à jour les mesures de sécurité et de les améliorer en tenant compte des incidents réels survenus et des risques de sécurité de l'information actuels et anticipésd'améliorer les moyens de maîtrise tout en prenant en compte les risques de l'organisation et les leçons tirées des incidents.

0.6 Normes0.7 Normes internationales associées

Alors que la présente Norme internationale propose des lignes directricesle présent document propose des recommandations portant sur un vaste éventail de mesures de sécurité liées à l'information d'utilisation courante dans nombre d'organisations différentes, les autres normesmoyens de maîtrise qui sont communément utilisés dans plusieurs organisations différentes, d'autres documents de la famille ISO/CEIIEC 27000 présententproposent des conseils complémentaires ou des exigences relatifs à d'autres aspects de l'ensemble du processus global de managementgestion de la sécurité de l'information.

Se reporter à l'ISO/CEIIEC 27000 pour une introduction générale aux systèmes de management de la sécurité de l'informationà la fois aux SMSI et à la famille de normesdocuments. L'ISO/CEIIEC 27000 présentefournit un glossaire, définissant de manière formelle la plupart des termes utilisés dans la famille de normesdes documents ISO/CEIIEC 27000, et décrit le domaine d'applicationpérimètre et les objectifs de chaque élément de cettemembre 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.

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

1 Domaine ~~d'application~~ d'application

~~La présente Norme internationale donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.~~

~~La présente Norme internationale est élaborée à l'intention des organisations désireuses~~

Le présent document fournit un ensemble de référence de moyens de maîtrise de l'information génériques, y compris des recommandations de mise en œuvre. Le présent document est conçu pour être utilisé par les organisations:

a) ~~de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre~~dans le contexte d'un système de ~~management~~gestion de la sécurité de l'information (SMSI) selon l'ISO/~~CEI~~IEC 27001;[10]

~~b) de mettre en œuvre des mesures de sécurité de l'information largement reconnues;~~

pour la mise en œuvre de moyens de maîtrise de l'information basés sur les bonnes pratiques reconnues au niveau international;

c) ~~d'élaborer leurs propres lignes directrices de management~~pour l'élaboration des recommandations de gestion de la sécurité de l'information spécifiques à une organisation.

2 Références normatives

~~Les documents suivants, en tout ou partie, sont référencés de manière normative dans le présent document et sont indispensables à son application. 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/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*~~

Le présent document ne contient aucune référence normative.

3 Termes ~~et définitions~~ , définitions et abréviations

~~Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 27000 s'appliquent.~~

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/