NORME ISO/IEC

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

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

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 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).

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.

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.

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.