Norme internationale

ISO/IEC 27017

Deuxième édition
2026-07

Sécurité de l'information, cybersécurité et protection de la vie privée — Contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

Numéro de référence
ISO/IEC 27017:2026(fr)

Document horizontal

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 documents. 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'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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*, en collaboration avec l'UIT-T (Recommandation UIT-T X.1631), et en collaboration avec le comité technique CEN/CLC/JTC 13, *Cybersécurité et protection des données* du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette deuxième édition annule et remplace la première édition (ISO/IEC 27017:2015 | Recommandation UIT-T X.1631:2015), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— le titre et le domaine d'application ont été modifiés;

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

— certaines mesures de sécurité ont été fusionnées, d'autres ont été supprimées, et plusieurs nouvelles mesures de sécurité ont été ajoutées.

Le présent document a obtenu le statut de document transversal conformément aux Directives ISO/IEC, Partie 1.

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.

Introduction

Les recommandations contenues dans le présent document s'inscrivent dans le prolongement de celles formulées dans l'ISO/IEC 27002 et les complètent.

Spécifiquement, le présent document fournit des recommandations appuyant la mise en œuvre des mesures de sécurité de l'information pour les clients de services en nuage (CSC) et les fournisseurs de services en nuage (CSP). Certaines recommandations sont destinées aux CSC qui assurent la mise en œuvre des mesures, tandis que d'autres sont destinées aux CSP afin de soutenir la mise en œuvre de ces mesures. La détermination des mesures de sécurité de l'information appropriées et l'étendue de l'utilisation des recommandations dépendent des résultats de l'appréciation du risque pertinente et de l'existence de toute exigence légale, contractuelle, réglementaire ou autre en matière de sécurité de l'information spécifique à l'informatique en nuage.

Sécurité de l'information, cybersécurité et protection de la vie privée — Contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

1 Domaine d'application

Le présent document fournit des recommandations pour les mesures de sécurité de l'information, fondées sur l'ISO/IEC 27002, qui sont applicables à la fourniture et à l'utilisation des services en nuage. Le présent document fournit:

— des recommandations supplémentaires concernant les mesures de sécurité pertinentes spécifiées dans l'ISO/IEC 27002:2022;

— des mesures de sécurité supplémentaires avec des recommandations spécifiquement liées aux services d'informatique en nuage.

Le présent document fournit des mesures de sécurité et des recommandations destinées aux clients de services en nuage (CSC) et aux fournisseurs de services en nuage (CSP).

Le présent document est pris en considération comme un document transversal, car il fournit une base et une vision commune de la sécurité en matière de disposition et d'utilisation des services en nuage.

NOTE Le présent document s'applique à tous les types de modèles de déploiement dans le nuage, y compris le nuage privé. Lors de l'application du présent document au nuage privé, les mesures et les recommandations du présent document sont applicables, bien que des ajustements puissent être nécessaires pour s'adapter aux relations et aux aptitudes des services internes d'un organisme.

2 Références normatives

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 22123-1, *Technologies de l'information — Informatique en nuage — Partie 1: Vocabulaire*

ISO/IEC 27002:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 27002, de l'ISO/IEC 22123-1 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/

3.1.1
aptitude
capacité à réaliser une activité spécifique

[SOURCE: ISO 19440:2020, 3.5]

3.2 Abréviations

API	interface de programmation d'application [*application programming interface*]
CSC	client de services en nuage [Cloud Service Customer]
CSN	partenaire de services en nuage [Cloud Service Partner]
CSP	fournisseur de services en nuage [Cloud Service Provider]
CSU	utilisateur de services en nuage [Cloud Service User]
DCP	données à caractère personnel
TIC	Technologies de l'Information et de la Communication
SaaS	logiciel en tant que service [Software as a Service]
DR	délai de rétablissement
IaaS	infrastructure en tant que service [Infrastructure as a Service]
PaaS	plateforme en tant que service [Platform as a Service]
OPR	objectif de point de rétablissement
SLA	accord de niveau de service

4 Recommandations pour l'utilisation du présent document

4.1 Relation entre le présent document et l'ISO/IEC 27002:2022

Le présent document fournit:

— des recommandations supplémentaires concernant les mesures de sécurité pertinentes spécifiées dans l'ISO/IEC 27002:2022;

— des mesures de sécurité supplémentaires avec des recommandations spécifiquement liées aux services d'informatique en nuage.

Le présent document fait référence aux attributs, aux mesures, aux objectifs, aux recommandations et aux autres informations figurant dans l'ISO/IEC 27002:2022, Articles 5 à 8. En raison de l'applicabilité générale de l'ISO/IEC 27002:2022, de nombreuses mesures, recommandations et autres informations s'appliquent à la fois au contexte général et au contexte de l'informatique en nuage d'un organisme. Par exemple, l'ISO/IEC 27002:2022, 5.3 «Séparation des tâches» prévoit une mesure qui peut être appliquée, que l'organisme agisse ou non en tant que CSP. Un CSC peut en outre tirer de la même mesure des exigences de séparation des tâches dans l'environnement informatique en nuage, par exemple en séparant les administrateurs des services en nuage des autres CSU.

Le présent document présente également les caractéristiques, les mesures, les objectifs, les recommandations et d'autres informations spécifiques aux services en nuage, destinées à atténuer les risques liés aux aspects techniques et opérationnels de ces services (voir 5.38, 5.39, 8.35 et 8.36). L'Annexe A présente

les correspondances entre l'ensemble des mesures du présent document et celles de l'édition précédente (ISO/IEC 27017:2015[1)]).

Les CSC et les CSP peuvent se référer à l'ISO/IEC 27002:2022 ainsi que le présent document identifier les recommandations relatives aux mesures générales et spécifiques aux services en nuage, le cas échéant. Ce processus peut être réalisé en effectuant une appréciation et un traitement du risque en matière de sécurité des informations dans le contexte organisationnel et opérationnel où les services en nuage sont utilisés ou fournis (voir 4.3.3).

4.2 Structure du présent document

Le présent document suit la structure utilisée dans l'ISO/IEC 27002:2022 pour la description des mesures.

Le présent document adapte les mesures de sécurité de l'information incluses dans l'ISO/IEC 27002:2022, Articles 5 à 8, afin de mieux s'appliquer à l'informatique en nuage. Comme dans l'ISO/IEC 27002:2022, la catégorisation des mesures donnée aux Articles 5 à 8 est appelée «thèmes» et les attributs de chaque mesure identifiés dans l'ISO/IEC 27002:2022 s'appliquent également.

Lorsque les mesures spécifiées dans l'ISO/IEC 27002:2022 sont applicables sans que les CSC et les CSP n'aient besoin d'informations supplémentaires, seule une référence à l'ISO/IEC 27002:2022 est fournie.

En plus des mesures de l'ISO/IEC 27002:2022, les mesures étendues des services en nuage sont accompagnées du préfixe «CLD» (mesures étendues des services en nuage). Lorsqu'une mesure spécifiée dans l'ISO/IEC 27002:2022 nécessite des recommandations supplémentaires spécifiques aux services en nuage liés à cette mesure, celles-ci sont fournies sous la forme de «recommandations pour les services en nuage». La préconisation est donnée selon l'un des deux types suivants:

— Type 1 (indiqué dans le Tableau 1), utilisé lorsqu'il existe des recommandations distinctes pour le CSC et le CSP;

— Type 2 (indiqué dans le Tableau 2), utilisé si la recommandation est la même pour le CSC et pour le CSP.

Tableau 1 — Type 1

CSC	CSP
Recommandations pour le CSC	Recommandations pour le CSP

Tableau 2 — Type 2

CSC	CSP
Recommandations pour le CSC et le CSP	

4.3 Concepts spécifiques à l'informatique en nuage

4.3.1 Relations avec les fournisseurs dans les services en nuage

Les 5.19 à 5.22 de l'ISO/IEC 27002:2022 fournissent les mesures, l'objectif de chaque mesure, des recommandations et d'autres informations pour gérer la sécurité de l'information dans les relations avec les fournisseurs. La prestation et l'utilisation de services en nuage est similaire à la relation avec les fournisseurs où le CSC est un acquéreur, et le CSP un fournisseur. Par conséquent, les 5.19 à 5.22 de l'ISO/IEC 27002:2022 s'appliquent aux CSC et aux CSP.

Les CSC et les CSP peuvent également former une chaîne d'approvisionnement. Par exemple, un CSP fournit un service en nuage de type aptitudes d'infrastructure. En plus de ce service, un autre CSP peut fournir un service en nuage de type aptitudes d'application. Dans ce cas, le second CSP agit en tant que CSC pour le premier et en tant que CSP pour le CSC qui utilise ses services. Dans ce scénario, l'organisme joue à la fois le rôle de CSC et de CSP. Il convient que chaque organisme prenne en compte les mesures qui lui sont

1) Annulée et remplacée par le présent document (ISO/ IEC 27017:2026).

applicables dans ses rôles de CSC et de CSP. Cet exemple illustre le cas où le présent document s'applique à un organisme à la fois en tant que CSC et en tant que CSP. Étant donné que les CSC et les CSP forment une chaîne d'approvisionnement par le biais de la disposition et de l'utilisation du service en nuage, le 5.21 de l'ISO/IEC 27002:2022, s'applique, car il traite de la gestion de la sécurité de l'information dans la chaîne d'approvisionnement des TIC.

La série ISO/IEC 27036 fournit à l'acquéreur et au fournisseur de produits et de services des recommandations détaillées concernant la sécurité de l'information dans les relations avec les fournisseurs. L'ISO/IEC 27036-4 traite directement de la sécurité de l'information des services en nuage dans les relations avec les fournisseurs. L'ISO/IEC 27036-4 s'applique également aux CSC en tant qu'acquéreurs et aux CSP en tant que fournisseurs.

4.3.2 Relations entre les CSC et les CSP

Dans l'environnement de l'informatique en nuage, les données des CSC sont stockées, transmises et traitées par un service en nuage. Par conséquent, les processus métier d'un CSC peuvent dépendre de la sécurité des informations du service en nuage. Sans un contrôle suffisant sur le service en nuage, il peut être nécessaire que le CSC prenne des précautions supplémentaires concernant ses pratiques en matière de sécurité de l'information.

Avant d'entrer en relation avec un fournisseur, le CSC est censé choisir un service, en tenant compte des écarts possibles entre les exigences en matière de sécurité de l'information du CSC et les aptitudes du service en matière de sécurité de l'information. Une fois qu'un service en nuage est sélectionné, il convient que le CSC gère l'utilisation du service en nuage de sorte à répondre à ses propres exigences en matière de sécurité de l'information. Dans cette relation, un effort de collaboration entre le CSC et le CSP autour de l'utilisation et de la fourniture du service en nuage est nécessaire afin que le CSC atteigne ses objectifs en matière de gestion de la sécurité de l'information. Cela comprend le partage des rôles et responsabilités entre le CSC et le CSP. Il convient que le CSP fournisse les informations et l'assistance technique nécessaires pour répondre aux exigences du CSC en matière de sécurité de l'information. Lorsque les mesures de sécurité de l'information fournies par le CSP sont prédéfinies et ne peuvent pas être modifiées par le CSC, il est possible que ce dernier mette en œuvre certaines de ses propres mesures afin d'atténuer les risques. De plus amples informations sur l'attribution des rôles partagés et responsabilités sont disponibles dans le document 5.38.

Il est important de comprendre qu'il existe des modèles de déploiement en nuage différents qui sont utilisés dans les environnements de l'informatique en nuage. Certains des modèles de déploiement en nuage comprennent:

— nuage privé;

— nuage public;

— multi-nuage;

— nuage fédéré;

— nuage hybride;

— multi-nuage hybride;

— inter-nuage.

Trois approches fondamentales peuvent être adoptées dans ces différents modèles de déploiement en nuage.

— Le CSC contrôle et gère les services en nuage qui sont fournis par chacun des CSP, y compris leur orchestration dans une solution en nuage (par exemple, modèle multinuage);

— Un CSP combine les services en nuage de plusieurs CSP avec des degrés variables d'activités d'orchestration, de contrôle et de gestion (par exemple, modèle internuage);

— Plusieurs CSP forment un partenariat dans le cadre d'une collaboration hors bande et partagent leurs ressources pour créer des services en nuage (par exemple, un nuage fédéré qui utilise un système de gestion d'une fédération de services en nuage pour orchestrer l'accès aux ressources des CSP).

Il est important de noter que ces approches ne sont pas mutuellement exclusives et qu'il est possible de les combiner. Une explication supplémentaire de ces modèles de déploiement en nuage est disponible dans l'ISO/IEC 5140.

4.3.3 Gestion des risques relatifs à la sécurité de l'information dans les services en nuage

Il convient que les CSC et les CSP disposent tous deux de processus de gestion des risques liés à la sécurité de l'information. Ils peuvent se référer à l'ISO/IEC 27001 pour les exigences relatives à la gestion des risques dans leurs systèmes de gestion de la sécurité de l'information, et à l'ISO/IEC 27005 pour des recommandations supplémentaires concernant la gestion des risques de sécurité de l'information en elle-même. L'ISO 31000, sur laquelle l'ISO/IEC 27001 et l'ISO/IEC 27005 sont alignées, peut également contribuer à la compréhension générale de la gestion des risques.

Les mesures et les recommandations fournissent aux CSC:

— des recommandations sur les mesures de sécurité de l'information associées à l'utilisation des services en nuage;

— des recommandations sur les informations et les aptitudes des services en nuage à obtenir auprès des CSP.

Les mesures et les recommandations couvrent également la manière dont les CSP peuvent fournir des informations et des aptitudes dans le cadre des services en nuage afin de soutenir les CSC dans leur gestion des risques liés à la sécurité de l'information. Les informations et les aptitudes peuvent être fournies dans des accords et d'autres documents disponibles pour les CSC.

5 Recommandations spécifiques au service en nuage relatives aux mesures organisationnelles

5.1 Politiques de sécurité de l'information

Les attributs, la mesure, l'objectif, les recommandations et les informations supplémentaires fournies dans l'ISO/IEC 27002:2022, 5.1, s'appliquent. Par ailleurs, les recommandations suivantes présentées dans le Tableau 3 ainsi que d'autres informations relatives aux services en nuage s'appliquent également.

a) Recommandations pour les services en nuage

Tableau 3 — Recommandations pour les politiques de sécurité de l'information

CSC	CSP
Il convient de définir une politique de sécurité de l'information concernant l'utilisation des services en nuage sous la forme d'une politique portant sur le thème spécifique du CSC. Il convient que la politique de sécurité de l'information du CSC soit cohérente avec les niveaux acceptables de risques liés à la sécurité de l'information définis par l'organisme pour ses informations et autres actifs associés. Lors de la définition de la politique de sécurité de l'information pour l'utilisation des services en nuage, il convient que le CSC tienne compte des éléments suivants: — les informations stockées dans l'environnement informatique en nuage soumises à l'accès et à la gestion par le CSP; — les actifs maintenus dans l'environnement informatique en nuage, par exemple les instances de machines virtuelles, les compartiments de stockage en nuage; — les processus exécutés sur un service en nuage virtualisé, en multilocation; — le niveau d'accès des CSU et le contexte dans lequel ils utilisent le service en nuage; — les administrateurs du service en nuage du CSC qui disposent de privilèges d'accès; — les emplacements géographiques de l'organisme du CSP et les pays dans lesquels le CSP peut stocker et traiter les données du CSC ainsi que les données obtenues à partir des services en nuage (même temporairement); — la possibilité d'utilisations non autorisées de services en nuage.	Il convient de définir des règles relatives à la fourniture du service en nuage afin d'appuyer la sécurité de l'information du CSC, de traiter la fourniture et l'utilisation de ses services en nuage en tenant compte des éléments suivants: — les exigences de référence en matière de sécurité de l'information applicables à la conception et à la mise en œuvre du service en nuage; — la multilocation et l'isolement des CSC; — la virtualisation des ressources, y compris les serveurs, les conteneurs et les réseaux; — l'accès du personnel du CSP aux données du CSC et aux données obtenues à partir des services en nuage; — les procédures de contrôle d'accès, par exemple authentification stricte pour l'accès administratif aux services en nuage; — la gestion du cycle de vie des comptes du CSC; — la communication aux CSC dans le cadre de la gestion du changement; — la communication des violations et des lignes directrices en matière de partage d'informations afin de faciliter les enquêtes et la criminalistique.

b) Autres informations pour les services en nuage

La politique de sécurité de l'information relative à l'utilisation des services en nuage du CSC est l'une des politiques portant sur des thèmes spécifiques décrites dans l'ISO/IEC 27002:2022, 5.1. La politique de sécurité de l'information d'un organisme porte sur ses informations et ses processus métier. Lorsqu'un organisme utilise des services en nuage, il peut avoir une politique pour l'informatique en nuage en tant que CSC. Les informations d'un organisme peuvent être stockées et maintenues dans l'environnement informatique en nuage, et les processus métier prendre en compte l'environnement informatique en nuage. Les exigences générales en matière de sécurité de l'information définies dans la politique de sécurité de l'information au niveau supérieur sont suivies par la politique portant sur des thèmes spécifiques qui régit l'utilisation des services en nuage.

En revanche, les règles pour la fourniture de services en nuage traitent des informations et des processus métier des CSC, et non des informations et des processus métier du CSP. Il convient que la règle traite de la sécurité de l'information dans l'environnement de service en nuage et de la fourniture de fonctions et d'informations venant à l'appui de la sécurité de l'information des CSC. Il convient que les exigences en matière de sécurité de l'information pour la fourniture de services en nuage répondent à celles des CSC potentiels.

La virtualisation des ressources dans le cadre de l'informatique en nuage comporte plusieurs aspects qui peuvent avoir des répercussions sur la sécurité de l'information du CSC. Voici quelques exemples de ces aspects:

— gestion du cycle de vie des instances virtuelles;

— gestion de l'utilisation d'images virtualisées;

— gestion des instances virtuelles inactives ou hors ligne;

— caractéristiques des instantanés;

— contrôler l'utilisation des portails en libre-service;

— protection des hyperviseurs.

5.2 Rôles et responsabilités liées à la sécurité de l'information

Les attributs, la mesure, l'objectif, les recommandations et les informations supplémentaires fournies dans l'ISO/IEC 27002:2022, 5.2, s'appliquent. En outre, les recommandations figurant dans le Tableau 4 ainsi que d'autres informations relatives aux services en nuage s'appliquent également.

a) Recommandations pour les services en nuage

Tableau 4 — Recommandations pour les rôles et responsabilités en matière de sécurité de l'information

CSC	CSP
Il convient que le CSC définisse les rôles et responsabilités en matière de sécurité de l'information pour l'utilisation des services en nuage et qu'il les documente dans les politiques et procédures portant sur le thème spécifique. Il convient que le CSC attribue les rôles et responsabilités, et qu'il en informe les CSU concernés.	Il convient que le CSP définisse et attribue les rôles et responsabilités en matière de sécurité de l'information qui sont liés à la fourniture des services en nuage.

b) Autres informations pour les services en nuage

L'ISO/IEC 22123-3 définit les rôles et les sous-rôles du CSC et du CSP.

5.3 Séparation des tâches

Les attributs, la mesure, l'objectif, les recommandations et les informations supplémentaires fournies dans l'ISO/IEC 27002:2022, 5.3, s'appliquent.

5.4 Responsabilités de la direction

Les attributs, la mesure, l'objectif, les recommandations et les informations supplémentaires fournies dans l'ISO/IEC 27002:2022, 5.4, s'appliquent.

5.5 Relations avec les autorités

Les attributs, la mesure, l'objectif, les recommandations et les informations supplémentaires fournies dans l'ISO/IEC 27002:2022, 5.5, s'appliquent.

5.6 Relations avec des groupes de travail spécialisés

Les attributs, la mesure, l'objectif, les recommandations et les informations supplémentaires fournies dans l'ISO/IEC 27002:2022, 5.6, s'appliquent.