

# ISO/IEC 27001 : 2022

## Système de Management de la Sécurité de l'Information

### Fiche d'information



#### Ce que vous devez savoir

ISO/IEC 27001 est la norme ISO pour un système de management de la sécurité de l'information (SMSI). Les entreprises qui obtiennent la certification ISO/IEC 27001 sont conformes en matière de protection des informations et des risques associés à la protection des données digitales.

ISO a annoncé que la norme ISO/IEC 27001 :2013 est remplacée par ISO/IEC 27001 :2022. Cette nouvelle version est basée sur les changements apportés à la norme ISO/IEC 27002, qui est le guide de support détaillant comment les entreprises sont tenues de se conformer aux contrôles de l'annexe A de ISO/IEC 27001.

ISO a publié les dernières modifications de ISO/IEC 27002 :2022 le 15 février 2022, et l'annexe A de ISO/IEC 27001 a été revue afin de s'aligner sur les nouvelles modifications de ISO/IEC 27002. La nouvelle norme ISO/IEC 27001 a été publiée le 25 octobre 2022, en anglais.

Des modifications ont été apportées à la norme ISO/IEC 27001, spécifiquement au niveau des contrôles de l'annexe A de ISO/IEC 27001 afin de refléter les changements de la norme ISO/IEC 27002 :2022

Le nouvel intitulé de la norme ISO/IEC 27002 :2022 est Sécurité de l'information, Cybersécurité et Protection de la vie privée – Système de Management de la sécurité de l'information.

#### Quelles sont les modifications apportées à la norme ISO/IEC 27001 ?

##### Les catégories de contrôles

Les contrôles ont été mis à jour et sont passés de 114 à 93, répartis en quatre catégories : Organisations, liés au personnel, physiques et technologiques.

- 58 contrôles restent en place avec la mise à jour
- 24 contrôles ont été fusionnés
- 11 contrôles ont été ajoutés

La sécurité du cloud est un nouveau sujet désormais pris en compte dans la norme ISO 27001 :2022.

La norme ISO/IEC 27002 :2022 fournit désormais une structure plus transparente de contrôles qui peuvent être appliqués dans l'ensemble de votre entreprise. Les contrôles fournissent désormais des aspects plus techniques de la cybersécurité et des facteurs humains en matière de protection de la vie privée.

##### Les critères

Des critères ont été introduits dans chaque contrôle. Les critères de la norme ISO/IEC 27001 permettent aux entreprises de créer différents points de vue, c'est-à-dire différentes catégorisations des contrôles vus sous un angle différent du thème ; en d'autres termes, les entreprises peuvent ainsi orienter les contrôles vers les bonnes cibles.

Les entreprises peuvent créer leurs propres critères. Chaque critère énuméré ci-dessous est accompagné d'une série de critères correspondants.

- Types de contrôle
- Propriétés de la sécurité de l'information
- Concepts de cybersécurité
- Capacités opérationnelles
- Domaine de sécurité

##### Vous êtes déjà certifié ISO/IEC 27001 ?

Votre entreprise va avoir 3 ans pour effectuer la transition vers la nouvelle version de la norme.

IMSM est spécialisé dans les services de transitions de vos systèmes depuis plus de 25 ans et propose un forfait de transition complet, à prix fixe et à valeur ajoutée garantie. Afin d'étudier les meilleures options ouvertes à vous pour planifier la transition de votre système, contactez-nous pour une consultation gratuite.



Contactez-nous