PREVSÉCU

Santé et Sécurité au travail

SÉCURITÉ DE L'INFORMATION

L'ISO/IEC 27001, la norme internationale pour la sécurité de l'information

Le succès d'une organisation peut être mesuré aujourd'hui en fonction de la façon dont cette organisation traite l'information. A la fois la confidentialité des données personnelles, la disponibilité des systèmes informatiques et l'exactitude des informations financières sont cruciales pour tout type d'organisation: grande ou petite, entreprise ou gouvernement. Des exemples récents ont montré qu'aucune entreprise ou organisation n'est protégée contre d'éventuelles cyberattaques ou violations de données. Outre le fait qu'en tant qu'organisation vous risquez de perdre la confiance du client, cela peut également entraîner de graves préjudices financiers.

Que prévoit la norme ISO/IEC 27001 ?

Appelée « ISO/IEC 27001 : Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences », cette norme montre, à l'aide d'un ensemble d'exigences, comment établir, mettre en œuvre, évaluer et améliorer en permanence un SMSI efficace. L'objectif : protéger la confidentialité, la disponibilité et l'intégrité de toutes les données au sein de votre organisation.

L'ISO/IEC 27001 : 10 chapitres

Dans la dernière version, la structure de la norme ISO/IEC 27001 a été adaptée à la **High Level Structure (HLS)**. Des dizaines d'autres normes de management de l'ISO ont également subi la même transformation ces dernières années. L'ISO veille ainsi à ce qu'elles aient toutes la même structure de base uniforme. L'avantage ? Il est plus facile pour les organisations d'intégrer différentes normes dans un seul système de management. Par exemple, il est possible de mettre en place votre SMSI en combinaison avec les normes ISO 9001 (managementde la qualité), ISO 14001 (management de l'environnement) ou ISO 45001 (santé et sécurité au travail).

Plus concrètement, la HLS signifie, entre autres, que la norme ISO/IEC 27001 comporte les **dix chapitres** suivants :

1. Domaine d'application
2. Références normatives
3. Termes et définitions tels que définis dans la norme ISO/IEC 27000
4. Contexte de l'organisation
5. Leadership
6. Planification: risques et opportunités
7. Support du SMSI
8. Fonctionnement du SMSI
9. Évaluation des performances
10. Amélioration

ISO/IEC 27001: des mots de passe à la protection incendie

Les chapitres de la norme ISO/IEC 27001 traitent notamment des **thèmes** suivants :

- Règlementation (protection des données à caractère personnel)
- Organisation (rôles et responsabilités des collaborateurs)
- Ressources (infrastructures, réseaux et systèmes informatiques)
- Personnel (politique, erreurs humaines, vols, fraudes et autres abus)
- Sécurité physique (accès aux bâtiments ou à l'infrastructure informatique)
- Communication (gestion des systèmes, des processus et des procédures)
- Développement et maintenance de systèmes et de logiciels (documentation et processus)
- Continuité des affaires (politiques et procedures)

Pourquoi appliquer la norme ISO/IEC 27001 ?

Les principaux avantages de la norme ISO/IEC 27001 :

Protection des données cruciales : avec un SMSI, vous réduisez le risque que vos informations soient utilisées à mauvais escient, qu'elles soient incorrectes ou qu'elles ne soient plus disponibles à temps.
Clarté : des procédures opérationnelles écrites et une répartition claire des rôles vous permettent d'identifier systématiquement les vulnérabilités et de prendre en main de manière ciblée.
Confiance accrue des clients : les clients manifestent un intérêt croissant pour la manière dont leurs données sont gérées. Avec un SMSI, vous pouvez les rassurer et avoir la certitude qu'ils continueront à choisir votre organisation à l'avenir.
Risque financier réduit : le non-respect des lois pertinentes peut entraîner des amendes élevées. De plus une perte de réputation et une perte de clients peuvent entraîner de graves préjudices financiers.
Du sur mesure pour chaque organisation : la norme ISO/IEC 27001 est applicable à toute organisation, quels que soient son secteur, sa taille ou son type.
Renommée internationale : la norme de management ISO est connue dans le monde entier et renforce sensiblement votre crédibilité au-delà des frontières nationales.

À qui s'adresse la norme ISO/IEC 27001 ?

La sécurité de l'information et un SMSI efficace sont importants pour toutes les organisations. Chaque organisation ou entreprise garde une trace des flux d'informations physiques et/ou numériques.

Certificat ISO/IEC 27001

L'ISO/IEC 27001 est la norme internationale pour la sécurité de l'information par excellence. Elle se classe parmi les **4 normes de management ISO les plus populaires** si l'on considère le nombre de certifications. Selon la dernière étude ISO (2018), 59.934 sites dans le monde ont un certificat ISO/IEC 27001, dont 208 en Belgique.

Qu'est-ce qu'un certificat ISO/IEC 27001 ?

La mise en œuvre correcte et complète d'une norme de management ISO n'est **pas une obligation** pour les organisations. Vous pouvez, par exemple, appliquer une partie de la norme. Mais si vous visez la certification, vous devez remplir toutes les exigences que contient la norme. Dans ce cas, une **institution indépendante** évaluera votre

SMSI à votre demande. Si l'évaluation est positive, vous recevrez une preuve écrite attestant que vous répondez à toutes les exigences de la norme. Ce certificat est **valable 3 ans**. Vous passez ensuite par un nouveau processus de certification (si vous le souhaitez) pour en renouveler la validité.

Pourquoi tenter d'obtenir un certificat ISO/IEC 27001 ?

Les 3 principaux avantages d'un certificat ISO/IEC 27001 :

1. **De nouvelles opportunités commerciales** : tout le monde veut avoir la certitude à l'heure actuelle que ses données seront conservées en toute sécurité au sein de votre organisation. Un certificat inspire confiance aux clients.
2. **Un atout dans les appels d'offres** : les pouvoirs publics et les grandes entreprises qui lancent des appels d'offres recherchent de plus en plus des organisations qui offrent des garanties optimales en matière de sécurité de l'information.
3. **Une amélioration continue de votre sécurité de l'information** : obtenir et conserver un certificat impliquent que vous devez effectuer (ou faire effectuer) des audits périodiques. Cela signifie que vos objectifs et vos procédures sont toujours à jour.

Comment obtenir un certificat ISO/IEC 27001 ?

Bien que l'ISO, la CEI et le NBN facilitent l'élaboration de normes de management, ces organisations ne participent pas à leur certification. En d'autres termes, vous ne pouvez jamais faire certifier votre organisation par l'ISO, la CEI ou le NBN. Ce sont **des organismes de certification indépendants** qui délivrent les certificats à l'issue d'une évaluation positive.

Quels organismes délivrent des certificats pour l'ISO/IEC 27001 ?

En Belgique, il existe de nombreux organismes qui délivrent des certificats ISO/IEC 27001 après un audit de votre organisation. Cependant, tous ne sont pas accrédités par **BELAC, l'organisme d'accréditation belge**. Passer par un organisme accrédité n'est pas obligatoire, mais avec un acteur accrédité, vous aurez la garantie d'avoir été audité par des experts. L'accréditation est en effet une preuve d'impartialité, d'indépendance et de compétence technique.

Certification ISO/IEC 27001 : plan par étape

Vous prévoyez de faire certifier votre système de management de la sécurité de l'information ? Il est conseillé de suivre les étapes suivantes :

1. **Soutien** : L'adhésion des dirigeants est sine qua non. Ce n'est que lorsqu'ils soutiendront l'idée que vous pourrez entamer la démarche.
2. **Achat de la norme NBN EN ISO/IEC 27001:2017** : Rendez-vous dans l'e-shop du NBN.
3. **Formation** : Qu'ils soient débutants ou expérimentés, les utilisateurs d'une norme tireront profit d'une formation. Ne manquez pas de consulter la page de présentation des formations ISO/IEC 27001 proposées par NBN Learning Solutions.
4. **Mesure de référence** : Effectuez une mesure de référence vous-même, avec vos collègues ou en collaboration avec un consultant externe. Cette analyse GAP de la situation actuelle et de la situation souhaitée vous montrera où se situent les principaux points à travailler.
5. **Préparation** : Sur la base de l'analyse préalable, élaborez un plan par étape avec des objectifs concrets pour votre organisation et la direction. Établissez un calendrier et, si nécessaire, désignez des équipes de projet avec une répartition des tâches claire.
6. **Communication** : Communiquez votre plan aux parties prenantes les plus importantes afin que tout le monde soit sur la même longueur d'onde. Cela facilitera la mise en œuvre de la norme de management.
7. **Mise en œuvre** : Réaliser toutes les actions prédéfinies et travailler (progressivement) à la mise en œuvre complète de la norme de management.
8. **Audit interne** : Dès que votre SMSI est prêt, effectuez un audit interne pour voir si vous êtes entièrement prêt pour l'audit officiel (externe). Cet audit interne est une étape obligatoire dans l'obtention du du certificat et vous pouvez le faire vous-même ou en collaboration avec un prestataire de services externe.
9. **Audit de certification** : Contactez un organisme de certification pour un audit. Préparez-le bien en discutez ensemble après l'audit des lacunes éventuelles et de la manière dont vous pouvez y remédier.
10. **Certification** : Si votre organisation remplit toutes les exigences de la norme, vous recevrez un certificat. Il est bien sûr prévu que vous continuiez à travailler sur votre SMSI après la certification.

Selon la taille et la complexité de votre organisation, le délai d'exécution de ce plan par étape est **de 3 mois à 1 an**. Votre préparation, votre compréhension des exigences spécifiques de la norme et le niveau de maturité de votre organisation seront déterminantes.

Certification ISO/IEC 27001 : le coût

Le coût dépend de plusieurs facteurs. Par exemple, êtes-vous entièrement responsable du système de gestion de la sécurité de l'information ou êtes-vous encadré par un partenaire externe ? La taille et la complexité de votre organisation jouent également un rôle. Vous devez en tout cas faire appel à un organisme de certification pour effectuer les audits. En principe, vous concluez un **contrat de 3 ans** avec lui, soit la durée de validité d'un certificat.

Audit externe ISO/IEC 27001

Il est important de savoir que vous déterminez vous-même le champ d'application de la certification – et donc des audits. Cela vous permet de choisir d'inclure certains services et pas d'autres dans le champ d'application. Le SMSI du ou des services pour lesquels vous souhaitez être certifié est ensuite évalué dans le cadre d'un audit par un organisme de certification indépendant. Avant ces audits officiels, vous pouvez également organiser des audits internes pour vous y préparer.

Comment se déroule un audit externe ?

À partir de 3 mois après la mise en œuvre complète de la norme de management, vous pouvez entamer le processus de certification et programmer un audit externe. Selon la taille de votre organisation, cet audit prendra un ou plusieurs jours. Si vos services sont répartis sur plusieurs sites, l'auditeur visitera toutes les installations.

L'audit comporte **deux phases** :

- phase 1 : un contrôle approfondi de tous les documents nécessaires
- phase 2 : une analyse (sur place) du fonctionnement du SMSI

Que se passe-t-il après l'audit ?

Après l'audit, l'organisme de certification décide si vous avez correctement mis en œuvre votre système de gestion. En cas d'avis négatif, vous recevrez un rapport avec les non-conformités et les points sur lesquels vous devez travailler. Dans ce cas, un audit supplémentaire apportera une réponse définitive. En cas d'avis positif, vous obtiendrez un certificat. L'auditeur vous rendra ensuite visite chaque année pour évaluer votre SMSI. Vous pouvez demander le renouvellement de votre certificat tous les 3 ans – le délai de validité d'un certificat.

Norme de la famille ISO/IEC 27000

Bien que la norme **ISO/IEC 27001 soit la seule norme certifiable** de la série ISO/IEC 27000, il peut être utile de la mettre en œuvre en combinaison avec d'autres normes de la même famille. Celles-ci indiquent comment appliquer la norme ISO/IEC 27001 et renforcer votre SMSI. Il s'agit concrètement des normes suivantes :

NBN EN ISO/IEC 27000:2017 - **Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire :** cette norme donne un aperçu de la terminologie essentielle utilisée dans l'ensemble de la série de normes. En outre, la norme ISO/IEC 27000 montre comment les autres normes sont liées entre elles.
NBN EN ISO/IEC 27002:2017 - **Technologies de l'information - Techniques de sécurité - Code de pratique pour le management de la sécurité de l'information** : fournit une image détaillée des mesures que vous pouvez prendre pour répondre aux exigences de la norme ISO/IEC 27001.
NBN ISO/IEC 27018:2019 - **Technologies de l'information - Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant**

comme processeur de PII : cette norme vous permet d'assurer la sécurité des informations personnelles identifiables dans un nuage public, comme Microsoft365, SalesForce et Gmail.

NBN ISO/IEC 27701:2019 **- Techniques de sécurité - Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée - Exigences et lignes directrices** : l'outil par excellence pour un système de gestion des informations personnelles (SGIP). Vos données numériques sont ainsi toujours protégées.