En clair, grâce à elle, les entreprises surveillent, révisent, entretiennent et améliorent la gestion de la sécurité des informations en mettant en place un Système de Management de Sécurité de l'Information (SMSI).

9 étapes de mise en place de la norme ISO 27001

Sophie Meunier 4th juillet 2018

Il existe de nombreuses raisons d'adopter la norme ISO 27001, norme internationale décrivant les bonnes pratiques à suivre pour les systèmes de gestion de la sécurité de l'information (SMSI). Elle aide les organisations à améliorer leur sécurité, à se conformer aux règlementations de cyber sécurité et à protéger et améliorer leur réputation.
Mais la mise en place de la norme prend beaucoup de temps et d'efforts. Cela doit être évident, au moins si vous croyez en la phrase « Rien de ce qui vaut la peine n'arrive sans effort ». Nous avons rendu le processus plus simple en le divisant en neuf étapes.

1. Contenu de la mission

Le projet de mise en place doit commencer par la désignation d'un leader de projet, qui travaillera avec d'autres membres du personnel. Il s'agit essentiellement d'un ensemble de réponses aux questions suivantes :

- Qu'espérons-nous réaliser ?
- Combien de temps cela prendra-t-il ?
- Qu'est-ce que cela coutera ?
- Avons-nous le soutient des équipes de direction ?

2. Initiation du projet

Les organisations doivent utiliser leur contenu de mission afin de construire une structure plus définie et plus détaillée concernant les objectifs liés à la sécurité de l'information et l'équipe gérant le projet, la planification et les risques.

3. Initiation du SMSI

La prochaine étape est d'adopter une méthodologie de mise en place d'un SMSI. La norme ISO 27001 reconnait que la démarche d'amélioration continue suivant une approche par processus est le modèle le plus efficace pour la gestion de la sécurité de l'information.

Cependant, elle ne précise aucune méthodologie en particulier et permet aux organisations d'utiliser la méthode de leur choix ou de continuer avec le modèle déjà en place.

4. Cadre de gestion

A ce stade, le SMSI aura besoin d'une signification plus large du cadre. Cela comprend l'identification de la portée du système, qui dépendra du contexte. La portée doit également prendre en compte les appareils mobiles et les télétravailleurs.

5. Critères de sécurité

Les organisations doivent identifier leurs principaux besoins de sécurité. Il s'agit des exigences et mesures correspondantes ou des contrôles nécessaires pour gérer l'entreprise.

6. Gestion des risques

La norme ISO 27001 permet aux organisations de définir de manière plus large leurs propres processus de gestion des risques. Les méthodes les plus communes sont axées sur les risques liés à des actifs précis ou les risques présentés dans des scénarios précis. Les points positifs et négatifs de chacun et certaines organisations seront plus en mesure d'utiliser l'une ou l'autre des méthodes.

L'analyse des risques ISO 27001 comprend cinq points importants :

- Etablir un cadre d'analyse des risques
- Identifier les risques
- Analyser les risques
- Evaluer les risques
- Sélectionner les options de gestion des risques

7. Plan de traitement des risques

Il s'agit du processus de construction des contrôles de sécurité ayant pour but de protéger les informations d'une organisation. Afin de garantir l'efficacité de ces contrôles, on doit vérifier que les employés sont capables d'opérer et d'interagir avec les contrôles, et qu'ils connaissent leurs obligations en matière de sécurité de l'information.

On developpe également un processus vous permettant de déterminer, réviser et maintenir les compétences nécessaires afin d'atteindre vos objectifs en matière de SMSI. Cela comprend la mise en place d'analyses et la définition d'un bon niveau de compétence.

8. Mesurer, contrôler et réviser

Pour qu'un SMSI soit utile, il doit répondre aux objectifs de sécurité de l'information. Les organisations doivent mesurer, contrôler et réviser la performance du système. Cela implique l'identification de métriques ou

d’autres méthodes permettant de juger l’efficacité et la mise en place des contrôles.

9. Certification

Une fois l’ SMSI en place, les organisations devraient essayer d’obtenir un certificat auprès d’un organisme de certification accrédité. Cela prouve aux parties prenantes que l’SMSI est efficace et que les organisations comprennent l’importance de la sécurité de l’information.

Le processus de certification implique la révision des documentations des systèmes de gestion de l’organisation afin de vérifier que les contrôles appropriés ont été mis en place. L’organisme de certification mènera également un audit sur-site afin de tester les procédures.

Comment obtenir la certification ISO ?

La **certification ISO** 9001 est délivrée par une organisme certificateur à l'issue d'un audit. L'entreprise doit au préalable s'y préparer et choisir l'organisme.
Le **certificat** est valable 3 ans, mais des audits annuels permettent de le maintenir.

Pourquoi être certifié ISO 27001 ?

La **certification ISO 27001** vous aide non seulement à démontrer vos bonnes pratiques de sécurité, rehaussant ainsi les relations professionnelles tout en fidélisant les clients existants, mais elle vous offre aussi un avantage marketing sur vos concurrents en vous assimilant à Google, Microsoft et Verizon.

Qui certifié ISO 27001 ?

la **certification iso 27001** permet de :

D'identifier et maitriser les risques de défaillance informatique, grâce à des audits cyber réalisés par des experts Bureau Veritas.

Quels sont les 4 critères de sécurité selon la norme ISO 27001 ?

La **norme ISO 27001** est un texte qui vise le contrôle, la **sécurité** et des services à travers la maîtrise de **4** paramètres. Assurer la disponibilité des informations et des services. Sécuriser l'intégrité des données critiques. Garantir la confidentialité des données sensibles ou des données clients.

Comment se certifier ISO 27001 ?

Pour obtenir la **certification ISO 27001**, vous devez : Réaliser une analyse de risques dans le contexte de l'entreprise. Identifier les moyens à mettre en œuvre et

les ressources à manager (formation du personnel). Définir une politique de sécurité et choisir le périmètre du SMSI.

C'est quoi la norme ISO 9001 ?

ISO **9001** définit les critères applicables à un système de management de la qualité.

Quel est le rôle de l'ISO ?

Les Normes **ISO** aident les entreprises de toutes tailles et de tous secteurs à réduire leurs coûts, accroître leur productivité et accéder à de nouveaux marchés.

Qu'est-ce que le SMSI ? Le **SMSI** désigne un ensemble de politiques et de processus visant à gérer la sécurité et à atténuer les risques, particulièrement pour la sécurité de l'information.

Les avantages de la certification ISO 27001

Mettre en place un SMSI visant à obtenir la certification ISO 27001 vous offre bien des avantages, non seulement pour le développement de votre activité, mais aussi en interne :

- **Gagner en crédibilité** sur votre marché. La certification ISO 27001 est un avantage concurrentiel et améliore votre réputation. Vos clients ont confiance en vous et vous restent fidèles. Mais c'est également un argument en votre faveur auprès de vos prospects.
- **Réduire vos coûts** en matière de sécurité. Cette certification vous permet d'identifier le bon SMSI à mettre en place et de supprimer toute autre mesure de sécurité inutile. Vous évitez également les pertes financières et pénalités associées aux violations des informations.
- **Faciliter les échanges à l'international** avec une certification reconnue par-delà les frontières.
- **Gagner en sécurité.** Vous identifiez efficacement les menaces de votre système d'information. Vous améliorez continuellement vos pratiques pour sécuriser les données. La mise en place en interne d'un système de management performant réduit les risques et mobilise votre personnel formé pour répondre aux exigences de la norme.
- **Être conforme à la réglementation** en matière de gestion des risques et de la sécurité (notamment au Règlement Général sur la Protection des Données – RGPD).

Cette certification iso 27001 atteste que :

- Vous savez identifier les menaces (cyber-attaques, vols ou pertes de données…).
- Vous maîtrisez les risques concernant les informations sensibles détenues par votre société.
- Vous avez mis en place des mesures de protection adaptées et efficaces pour garantir la confidentialité, l'intégrité et la disponibilité des données.
- Vous faites évoluer votre SMSI pour vous adapter en permanence aux nouveaux risques.
- Vous vous engagez à maintenir un niveau de sécurité maximal.

Les obligations après la certification ISO 27001

Votre entreprise a obtenu la certification ISO 27001 ? C'est une bonne nouvelle et une étape de franchie ! Mais **être certifié vous oblige à évaluer en continu les performances de votre entreprise en matière de sécurité de l'information.**
La certification est valable 3 ans au bout desquels elle peut être renouvelée. Chaque année, un auditeur externe s'assure que votre démarche est pérenne :

- 1re année : un audit complet
- 2e et 3e année : un audit de suivi.

A l'issue de ce cycle, l'auditeur changera et vous aurez la possibilité de choisir un autre organisme certificateur.