PREVSÉCU

Santé et Sécurité au travail

SYSTÈME DE MANAGEMENT DE SÉCURITÉ

Certification ISO 27001 : une norme internationale dédiée à la Sécurité des Systèmes d'Information (SMSI) des entreprises et organisations

La norme ISO 27001 est la norme de référence internationale en termes de système de management de la sécurité de l'information (SMSI). Elle permet d'aborder la sécurité des systèmes d'information par les risques et permet de répondre aux menaces grandissantes telles que :

- **La diffusion non autorisée et non maîtrisée d'informations confidentielles**. Une telle fuite de données pouvant être d'ordre intentionnelle (malveillance interne, attaque extérieure) ou non intentionnelle (défaut de protection, erreur humaine),

- **L'interruption d'activité** liée à une attaque extérieure (virus, malware), une défaillance matérielle ou encore un défaut de disponibilité des applicatifs utilisés par l'entreprise ou l'organisation concernée,

- **La perte partielle ou totale de données** critiques ou non critiques, conséquence des points évoqués ci-dessus.

La mise en place d'un Système de Management de la Sécurité des Systèmes d'Information permet à l'entreprise de s'assurer de la bonne appréciation des risques de sécurité de l'information dans son environnement propre et en fonction de la criticité des données qu'elle traite de ses parties prenantes (clients, fournisseurs, employés, partenaires…).

Le SMSI ou Le Système de Management de la Sécurité de l'Information regroupe alors les systèmes d'informations, les processus et les personnes qui sont concernées par les mesures de protection.

Quels sont les objectifs de la norme ISO 27001 ?

L'ISO 27001 a pour objectifs d'assurer l'entreprise et ses parties prenantes de sa capacité à identifier et à se protéger de de toute perte, vol ou altération de données. Elle permet donc à l'entreprise de se doter de dispositifs permettant de prévenir et de faire face aux menaces potentielles en assurant un système de gestion structuré et efficace.

La norme ISO 27001 à également pour objectifs de répondre aux besoins des clients, fournisseurs, prestataires en assurant une protection de leurs données. A ce titre la norme ISO 27001 est alors complétée par le respect des exigences des réglementations en matière de protection des données tels que le **RGPD en Europe** ou par la norme **ISO 27701, norme internationale dédiée à la protection des données.**

Quelles sont les exigences clefs de la norme ISO 27001 ?

- S'assurer de la **compréhension de son organisation et de son contexte ainsi que celles de ses parties intéressées** concernées par le système de management de la sécurité de l'information. Pour cela les exigences et besoins de chaque partie intéressée doit être clairement établie,

- **Etablir et mettre en œuvre un Système de Management de la Sécurité de l'Information**, le tenir à jour et l'améliorer en continue en se basant sur les retours d'expérience et l'état de l'art très fortement évolutif en matière de sécurité informatique.
A ce titre la norme ISO 27001 est basée sur l'architecture HLS (High Level Structure) promu par l'ISO (International Standard Organisation) afin de favoriser l'intégration de plusieurs normes systèmes telles que l'ISO 9001 ou l'ISO 14001.

- **Garantir l'implication de la direction (Leadership SMSI)** est alors fondamentale pour assurer que le Système de Management de la Sécurité du Système d'Information corresponde bien à un axe stratégique fort et bien entendu afin que les ressources nécessaires soient allouées de manière dimensionnées aux objectifs et aux risques identifiés.

- **Identifier et traiter de manière proportionnée les risques et opportunités** afin de s'assurer que le système de management de la sécurité de l'information dispose des moyens de maîtrise suffisants ou qu'il permette d'établir les plans d'actions sécurité (PSSI : Plans de Sécurité des Systèmes d'Information),

- **Définir ses objectifs de sécurité de l'information** en veillant à la cohérence avec sa politique de sécurité et les risques effectivement identifiés. Ces objectifs devront être mesurables et permettre d'identifier et de prioriser les efforts de l'entreprise en matière de sécurité de l'information,

- **Planifier ses plans d'action en matière de sécurité informatique** et de sécurité de l'ensemble de ses systèmes d'information, à ce titre les contrôles opérationnels doivent être définis et suivis. Ainsi les risques et menaces sont identifiés et traités avec des actions proportionnées aux menaces,

- **Évaluer l'efficacité de son SMSI** au travers d'audits ou de tests de son niveau de sécurité du Système d'Information.

Quel doit être le périmètre du Système de Management du Système d'Information selon l'ISO 27001 ?

Le Système de Management de Sécurité de l'Information doit couvrir à la fois les risques liés à la gestion des infrastructures que ceux liés à la gestion des applicatifs. Il doit également s'attacher à réduire l'impact des menaces extérieures et celles des malveillances ou inattentions internes. Ainsi le SMSI doit couvrir sans s'y limiter les aspects suivants :

- **L'organisation interne :** fonctions et responsabilités liées à la sécurité de l'information, séparation des tâches, relations avec les autorités, la sécurité de l'information dans la gestion des projets lancés dans l'entreprise,

- **Appareils mobiles et télétravail :** Politique en matière d'appareils mobiles, télétravail : accès et partage des informations hors de l'entreprise,

- **Sécurité des ressources humaines avant l'embauche** (sélection des candidats, termes et conditions d'embauche), pendant la durée du contrat (responsabilité de la direction, Sensibilisation, apprentissage et formation à la sécurité de l'information, Processus disciplinaire), Rupture, terme ou modification du contrat de travail (Achèvement ou modification des responsabilités associées au
contrat de travail),

- **Gestion et responsabilité des actifs** : inventaire, propriété, utilisation correcte, restitution des actifs,

- **Classification et marquage de l'information**

- **Manipulation des supports :** gestion des supports amovibles, mise au rebut des supports, transfert physique des supports,

- **Contrôle des accès** : politique de contrôle d'accès, accès au réseau et aux services réseau,

- **Gestion des accès utilisateurs :** enregistrement et désinscription des utilisateurs, distribution des accès aux utilisateurs, gestion des droits d'accès à privilèges, gestion des informations secrètes d'authentification des utilisateurs, revue des droits d'accès utilisateurs, suppression ou adaptation des droits d'accès,

- **Responsabilité et contrôle d'accès des utilisateurs** : Utilisation d'informations secrètes d'authentification, Restriction d'accès à l'information, Sécuriser les procédures de connexion, Système de gestion des mots de passe, Utilisation de programmes utilitaires à privilèges, Contrôle d'accès au code source des programmes,

- **Mesures cryptographiques :** Politique d'utilisation des mesures cryptographiques, gestion des clefs,

- **Sécurité physique et environnementale :** Périmètre de sécurité physique, Contrôle d'accès physique, Sécurisation des bureaux, des salles et des équipements, Protection contre les menaces extérieures et
Environnementales, Travail dans les zones sécurisées, Zones de livraison et de chargement, sécurité des matériels,

- **Sécurité liée à l'exploitation :** protection contre les logiciels malveillant, sauvegarde, journalisation et surveillance, maîtrise des logiciels en exploitation, gestion des vulnérabilité techniques, audit du système d'information,
-

- **Sécurité des communications :** gestion de la sécurité des réseaux, transfert de l'information, acquisition, développement et maintenance des systèmes d'information, Sécurité des processus de développement et d'assistance technique,

- **Sécurité dans les relations avec les fournisseurs : gestion de la prestation de service,** chaîne d'approvisionnement des produits et des services informatiques,

- **Gestion des incidents liés à la sécurité de l'information et améliorations :** responsabilités et procédures, signalement des événements liés à la sécurité de l'information, signalement des failles
liées à la sécurité de l'information, réponse aux incidents liés à la sécurité de l'information, collecte de preuves,

- **Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité** : continuité de la sécurité de l'information, redondances,

Pourquoi se faire certifier ISO 27001 ?

La certification ISO 27001 permet à l'entreprise d'avoir un système fonctionnel et sécurisé dans le temps. Elle permet donc de réduire les coûts liés aux impacts potentiels des menaces et failles de sécurité auxquels l'entreprise est de plus en plus confrontée.

La CNIL propose une autoévaluation de maturité en gestion de la protection des données

La protection des données personnelles repose sur des activités mises en œuvre par chaque organisme (pilotage, gestion du registre, veille juridique, etc.). Toutefois, ces activités ne sont pas systématiquement prises en charge dans toutes les organisations et ne sont pas toujours gérées de manière homogène. La CNIL partage ses premières réflexions sur la réalisation d'un **« modèle de maturité » en gestion de la protection des données.**
Le modèle décrit 8 activités types liées à la protection des données en 5 niveaux de maturité. Des exemples d'actions ou productions illustrent chaque niveau de maturité pour chaque activité type sous forme de tableau.

Il permet aux organismes d'**évaluer leur propre niveau de maturité et de déterminer comment améliorer leur gestion de la protection des données.** Un plan d'actions pour combler les écarts constatés entre la pratique et le niveau adéquat ciblé par chaque organisme peut ainsi être élaboré sur cette base.

Cette méthodologie n'a pas pour objet d'assurer de fait la conformité. C'est un outil d'aide à l'analyse qui pourra contribuer à mettre en place des conditions favorables pour l'organisation des actions requises et les rendre pérennes, dans la logique de responsabilisation des acteurs.