Red-on-line

ISO 27001

GARANTIR LA SÉCURITÉ DES DONNÉES

SOMMAIRE

Nous sommes convaincus qu'entreprendre une démarche de certification afin d'améliorer continuellement la protection et la sécurité des informations est important. Red-on-line a initié la démarche de certification ISO 27001 en novembre 2021. Nous veillons à respecter strictement ces exigences en matière de sécurité dans notre organisation et pour nos clients.

INTRODUCTION

À l'heure où la digitalisation devient la norme dans les entreprises et les cyber attaques une menace réelle, la question de la sécurité des données s'impose comme une obligation pour la pérennité de l'activité. De nombreuses entreprises ont désormais compris l'importance de l'intégrité de leur data face à leurs utilisateurs, car elle touche directement à leur réputation. Des données qui fuient sont autant de clients ou partenaires susceptibles de perdre confiance.

Au cœur de cet enjeu, obtenir une certification s'inscrit dans une démarche volontariste. Elle prouve à la fois l'importance qu'une entreprise donne à la sécurité de son système de management de l'information (SMSI) et les moyens qu'elle met en œuvre pour y parvenir. Pour cela, la norme ISO/IEC 27001 vise à protéger vos données à travers des mesures déjà actives ou à mettre en place.
Dans ce document, vous en saurez plus sur cette norme ISO/IEC 27001 dédiée aux systèmes de management de la sécurité de l'information. En quoi consiste-t-elle ? Pourquoi est-il intéressant d'y prêter attention dans son organisation ou dans le choix de ses prestataires de services ? Quelles sont les étapes de certification ?

Pour finir, notre expert en Sécurité des Systèmes d'Information vous prodiguera quelques bonnes pratiques pour sécuriser votre organisation dans les meilleures conditions.

Ce document est coécrit avec Éric THIERRY, Responsable de la Sécurité des Systèmes d'Information du groupe Infopro Digital.

01 ISO/IEC 27001 : DÉFINITION ET PÉRIMÈTRE

RAPPEL

Les normes ISO couvrent l'intégralité des domaines certifiables, les normes IEC concernent uniquement les domaines de l'électricité, de l'électronique et de l'informatique comme une sous-catégorie des normes ISO.

La norme ISO/IEC 27001 atteste de la sécurité des données par la mise en place d'un système de management des systèmes d'information (SMSI). Suivre ses recommandations, sur le plan technique et humain, entre dans le champ de la protection des données internes et des tiers, et des bonnes pratiques techniques au sens large.

Comme toute norme de système de management, l'ISO 27001 permet aux organisations de s'améliorer en continu et d'aboutir à une performance complémentaire. Cette démarche (que l'on traduit par Plan / Do / Check / Act) est similaire à l'ISO 9001, ISO 14001, ISO 45001 ou ISO 50001 que vous connaissez d'ores et déjà. Comme elles, le suivi de la norme ISO 27001 et sa certification sont avant tout incitatifs et par conséquent non obligatoires.

PÉRIMÈTRE ET CHAMP D'APPLICATION DE LA NORME ISO 27001

Au sein du Système de Management des Systèmes d'Information, le périmètre de la certification porte à la fois sur les infrastructures, les personnes et les logiciels.

LE PÉRIMÈTRE QUE RED-ON-LINE SOUHAITE CERTIFIER :

- Conception, développement, maintenance et fourniture de logiciels et d'applications pour la gestion et la surveillance des risques liés à l'environnement, la santé et la sécurité (HSE) ;
- Fourniture de contenus juridiques pour la santé, la sécurité environnementale (HSE) et la sécurité alimentaire ;
- Fourniture de services de conseil et de formation.

02 POURQUOI SE FAIRE CERTIFIER ISO 27001 ?

Bien avant la crise sanitaire, dans ce que l'on appelle « le monde d'avant », la question de la **sécurité des données et des infrastructures était déjà un enjeu pour les entreprises**.

La pandémie, en accélérant la transformation digitale à marche forcée, a aussi eu pour effet de précipiter les attaques informatiques et d'entraîner des interrogations sur la gestion de la data.

Aujourd'hui, les entreprises privées comme les organismes publics et associatifs sont directement concernées par les attaques. **Les données valent de l'or** pour peu que l'on sache comment opérer. Elles représentent aussi une valeur importante pour les entreprises tant elles permettent désormais de s'appuyer dessus pour établir une stratégie de croissance dans l'ensemble des services (financier, marketing, relation client, etc.).

AINSI, LA NORME ISO 27001 A POUR BUT :

- D'assurer la confidentialité et la traçabilité de l'information au sein de l'organisation
- D'identifier les menaces et savoir y répondre avec les bons outils
- De maintenir l'intégrité de l'information et assurer sa disponibilité
- De respecter les exigences réglementaires et contractuelles
- De renforcer la confiance de ses clients et partenaires
- D'optimiser la gestion interne de la sécurité de l'information
- De maitriser les coûts de la cybersécurité

03 BÉNÉFICES DE L'ISO 27001

Les avantages concrets de l'ISO 27001 s'appliquent en premier lieu dans le travail des responsables de la sécurité informatique, et rejaillissent sur l'ensemble de l'entreprise. Ainsi, la mise en œuvre d'un SMSI 27001 et l'obtention de la certification maintiennent toute l'organisation dans une optique de sécurité et de disponibilité des données. Les démarches visant à la certification vous apportent ainsi :

- **La protection des données :** un SMSI garantit une organisation et des process renforcés en matière de sécurité de l'information.
  - La performance de l'organisation et des process en place est surveillée par la mise en place d'indicateurs et, périodiquement, par des audits internes.
  - L'audit de certification, réalisé annuellement par un organisme indépendant, valide que le niveau de performance souhaité est en conformité avec les objectifs fixés.

- **La clarté des informations :** Les process sont documentés à travers des procédures opérationnelles afin de clarifier l'organisation et d'identifier les rôles et responsabilités de chaque acteur impliqué dans la démarche.

- **La confiance :** Cette démarche renforce la confiance des parties intéressées (clients, sous-traitants, partenaires, fournisseurs, salariés…) dans la capacité de l'organisme à maitriser ses risques en matière de sécurité de l'information.

- **Le risque financier et réputationnel réduit :** À travers la connaissance et la maitrise des exigences légales, réglementaires et contractuelles, la démarche prévient les risques d'amendes très élevées pour non-respect de la sécurité des données de ses utilisateurs (ex : comme Free récemment qui été condamné par la CNIL à payer 300 000 € pour quatre manquements au RGPD sur les données de ses clients) ou de rupture de contrat. Dans le même temps, la réputation de l'entreprise n'est pas entachée par un manque de précautions.

- **L'amélioration continue :** Comme toute démarche de Système de management, l'ISO 27001 conduit l'organisme à s'améliorer de manière continue. À travers la fixation annuelle d'objectifs de performance adaptés aux ressources et aux besoins de l'organisation, l'organisme doit prouver sa capacité à progresser sur la prévention et la maitrise de ces risques.

04 LES ÉTAPES POUR SE FAIRE CERTIFIER

Vous envisagez également cette certification ?
Voici les étapes à suivre :

- Définition de la stratégie de la sécurité de l'information
- Lancement d'une démarche de gestion des risques
- Définition des objectifs et des indicateurs de sécurité
- Rédaction des politiques et procédures
- Sensibilisation des équipes

Dans le cadre d'une démarche de certification, il sera nécessaire de réaliser un audit à blanc avant de lancer l'audit de certification par un organisme indépendant. Cet audit de certification, réalisé sur un cycle de 3 ans, vous permettra de prouver que votre SMSI est conforme aux exigences de la Norme ISO 27001.

Quels sont les organismes accrédités pour certifier une entreprise ISO 27001 ?

D'après le site du COFRAC (Comité français d'accréditation), les organismes accrédités pour la certification du système de management de l'ISO 27001 sont :

- AFNOR CERTIFICATION
- LA SECURITE DES TECHNOLOGIES DE L'INFORMATION LSTI SAS
- LABORATOIRE NATIONAL DE METROLOGIE ET D'ESSAIS
- SGS INTERNATIONAL CERTIFICATION SERVICE
- VIGICERT

La France est 21ème au classement mondial en nombre de certifications (chiffres ISO survey 2020) avec 392 certificats (vs 21880 certificats ISO 9001 et 6458 certificats ISO 14001) (Source)

Selon l'AFNOR : la certification ISO/IEC 27001 a augmenté de 11 % en France en 2020 (après un bond de 57 % en 2019) et de 22 % dans le monde.

05 LES EXIGENCES DE CETTE NORME ISO27001

Comme dans toutes les normes ISO, celle-ci s'appuie sur les particularités de chaque organisation et donne des pistes qui s'adaptent en fonction des besoins et des risques inhérents à l'activité. Si bien que l'évaluation du périmètre d'action et de la gestion des risques de sécurité s'inscrivent au cœur des ambitions de l'ISO 27001.

Elle suppose par conséquent de :

- Définir le domaine d'application de votre SMSI (activités et zones géographiques)
- Identifier ses enjeux et les attentes de ses parties intéressées
- Analyser les risques en matière de sécurité de l'information
- Identifier les exigences légales et autres exigences applicables
- Identifier ses risques et ses opportunités en matière de SMSI
- Définir des objectifs et des plans d'action associés
- Sensibiliser et communiquer avec son personnel et les parties intéressées concernées (ex : partenaires, sous-traitants…)
- Documenter les process et les rôles et responsabilités des acteurs concernés
- Surveiller sa performance au travers de contrôle et d'indicateurs
- Réaliser des audits internes
- Gérer les dysfonctionnements et mettre en place des actions correctives
- Réaliser une revue de direction

06 LES 10 BONNES PRATIQUES À SUIVRE

01 TES MOTS DE PASSE, TU RENFORCERAS !

Utilisez des mots de passe complexes, de 8 caractères minimum, composés de majuscules, de minuscules, de chiffres et de caractères spéciaux. N'utilisez jamais les mêmes mots de passe pour vos usages personnels et professionnels. Ils doivent rester confidentiels.
Exemple : « 1f0Pro10Git@L »

02 TA SESSION, TU BLOQUERAS !

Ne laissez jamais votre session ouverte lorsque vous vous absentez. Votre poste de travail doit être verrouillé afin d'empêcher le vol de données et l'usurpation d'identité.
Verrouillage Windows : Touches + L -
Verrouillage Smartphone : verrouillage par modèle ou par mot de passe.

03 DES PÉRIPHÉRIQUES INCONNUS, TU TE MÉFIERAS !

Ne branchez pas de périphériques inconnus (clé USB, disque dur externe, smartphone...) sur votre poste informatique. Les risques et menaces associés sont principalement le vol d'informations et l'exécution automatique de codes malicieux. N'utilisez pas vos périphériques personnels dans vos activités professionnelles.

04 LE COURRIEL, TU FILTRERAS !

Une des attaques classiques, le « phishing », consiste à vous inciter à cliquer sur un lien contenu dans un mail, comme pour certaines publicités sur Internet. Ces liens peuvent être malveillants et vous voler des informations personnelles (mots de passe, n° CB) ou détruire vos documents.

05 LA NAVIGATION, TU PROTÈGERAS !

Soyez vigilant : Internet est une rue peuplée d'inconnus ! Ne donnez pas d'informations personnelles sur un site marchand ou bancaire, sans avoir vérifié au préalable que le site est sécurisé en « https » avec la présence du cadenas.

06 L'INFORMATION, TU NE DIVULGUERAS !

Méfiez-vous des questions et écoutes intrusives à des fins de récupération d'informations. Ne divulguez pas « accidentellement » des informations sensibles à une personne interne/ externe par téléphone, mail et/ou à l'oral.

07 TES SAUVEGARDES SUR LE RÉSEAU, TU FERAS !

La sauvegarde de vos données est une condition à la continuité de votre activité ! La défaillance du disque dur, la perte ou le vol de votre ordinateur sont toujours possibles. Pensez à enregistrer sur le réseau vos données professionnelles, elles sont sauvegardées toutes les nuits.

08 LES PORTES, TU FERMERAS !

Si vous disposez d'un badge d'accès, c'est avant tout pour interdire l'entrée d'inconnus dans les locaux. Tenir la porte, c'est aimable mais à condition de connaitre la personne que vous faites entrer ou si elle dispose d'un badge.

09 DE TON ANTIVOL, TU TE SERVIRAS !

La première brique de sécurité pour votre ordinateur portable est de minimiser le vol. Utiliser le câble antivol, toujours fourni, vous évitera de perdre vos données ainsi que votre environnement de travail et protégera également l'entreprise de ces potentielles fuites de données.

10 EN DÉPLACEMENT, SUR TES GARDES TU RESTERAS !

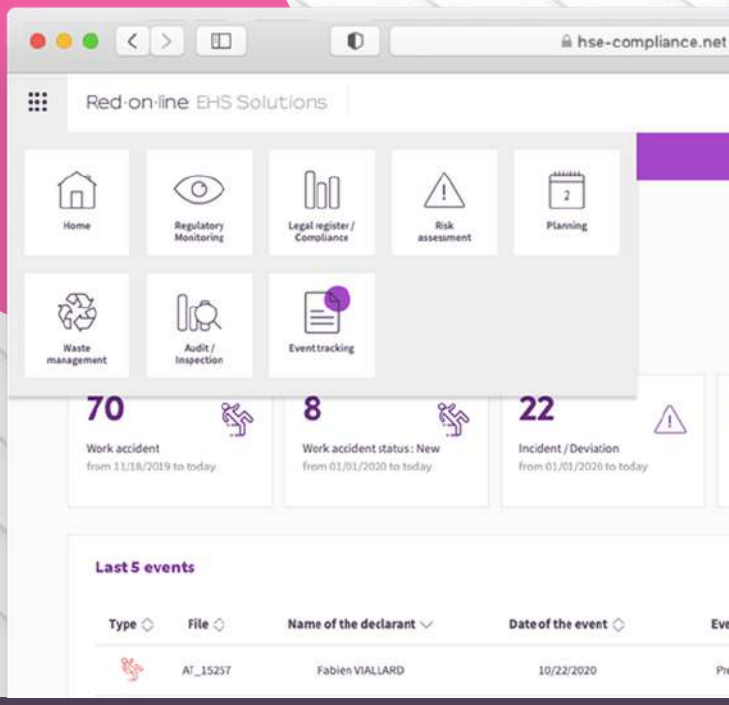
Lors de voyages professionnels des risques supplémentaires pèsent sur la sécurité des informations que vous emportez. Sachez que le WIFI des hôtels et lieux publics n'offr ent aucune garantie de confidentialité. Evitez de partir avec des données sensibles et gardez vos appareils, support et fichiers avec vous. Contactez le support informatique, il dispose de solutions de sécurité spécifiques pour vos déplacements (VPN, chiffrement,...).

Accompagner les systèmes de management

Nous proposons aux professionnels HSE, une offre leur permettant d'accompagner leur système de management et leur démarche de certification. Contactez-nous pour discuter de vos projets.

Red-on-line

L'association de l'expertise réglementaire et de la maîtrise technologique



Red-on-line solutions HSE :

- Veille et conformité réglementaire HSE
- Analyse des risques HSE
- Gestion des événements
- Accidentologie
- Suivi des indicateurs
- Objectifs et planification
- Audit et inspections

Votre partenaire pour la conformité et la maîtrise des risques en HSE

Contactez-nous pour que nous vous fassions une démo et que vous puissiez prendre en main la solution.

Red-on-line
Antony Parc II - 10, place du Général de Gaulle - 92 160 ANTONY
contact@red-on-line.com | www.red-on-line.com

Red-on-line