ISO 27001:2013

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences

Qu'est-ce que l'ISO 27001:2013 ?

L'ISO 27001 est la norme internationale qui fixe les exigences pour établir, mettre en œuvre, gérer et améliorer en permanence un système de management de la sécurité de l'information (SMSI) dans les organisations.

Cette norme offre aux organisations un modèle de meilleures pratiques permettant d'identifier, d'évaluer et de mettre en œuvre des contrôles pour gérer les risques de sécurité de l'information et protéger l'intégrité des données stratégiques des entreprises.

Pourquoi la certification ISO 27001:2013 est-elle si importante pour mon entreprise ?

Les informations sont parmi les ressources les plus précieuses et les plus stratégiques de n'importe quelle organisation. Dans le monde hyperconnecté qui est le nôtre aujourd'hui, les organisations sont exposées à des menaces de sécurité à grande échelle pour leurs informations et à des cyber-attaques destructrices, et ce quels que soient la taille, le secteur et la localisation des entreprises.

Si les systèmes de sécurité de l'information ne sont pas correctement gérés et mis à jour, les organisations courent le risque de subir de lourdes pertes financières et d'importantes atteintes à leur réputation.

Vérifier que votre organisation a mis en place les contrôles adéquats pour réduire les risques sérieux pour les données et éviter que les failles du système ne soient exploitées n'est plus une simple option.

Ces précautions sont encore plus incontournables depuis la publication du Règlement général sur la protection des données de l'UE, qui impose des exigences plus strictes et des amendes et sanctions plus lourdes aux organisations en cas de violation de données.

« Un système efficace fournit une protection contre les menaces connues et, plus important encore, contre les menaces inconnues. Cela nous oblige à examiner nos propres vulnérabilités et à nous demander si nous avons confiance en nos contrôles. »

Rob Acker
Directeur technique de la sécurité des informations de LRQA

Lloyd's Register LRQA

Améliorer la performance, réduire le risque

En quoi la certification ISO 27001:2013 peut-elle être bénéfique pour mon entreprise ?

- **Réduction des risques** : garantit que des contrôles sont en place pour réduire les risques de menaces de sécurité et éviter que les faiblesses des systèmes ne soient exploitées. Votre SMSI fait partie d'un plan de continuité d'activité, ce qui signifie que vous pouvez rétablir rapidement un fonctionnement normal en cas d'incident.
- **Meilleures pratiques** : ensemble de comportements et de mesures recommandant les meilleures pratiques à suivre en matière de gestion de la sécurité de l'information.
- **Conformité réglementaire** : la conformité exige de vous l'identification des procédures réglementaires applicables, pour un impact positif sur la gestion des risques et la gouvernance de l'entreprise.
- **Avantage concurrentiel** : la certification LRQA vous donne, ainsi qu'à vos clients, partenaires et autres intervenants importants, l'assurance que vous maîtrisez tous les risques de sécurité, y compris au niveau des personnes, des systèmes informatiques, des biens et, globalement, de la continuité de l'activité. La certification LRQA constitue une déclaration publique et indépendante de vos capacités qui peut vous servir en cas de réponse à des appels d'offres.
- **Intégration du système de management** : la norme repose sur le modèle PDCA (Plan, Do, Check, Act) que l'on retrouve dans d'autres normes relatives aux systèmes de management, ce qui simplifie le développement d'un système de management des activités unique répondant aux exigences d'autres normes.
- **Réduction des coûts** : en appliquant une méthode d'évaluation systématique des risques, vous consacrez toutes les ressources nécessaires à la réduction du risque global au lieu de ne regarder qu'un seul aspect du problème en laissant d'autres zones dans l'ombre.

Mieux vaut prévenir que guérir

Les informations sont parmi les ressources les plus précieuses et les plus stratégiques de n'importe quelle organisation. Dans le monde hyperconnecté qui est le nôtre aujourd'hui, les organisations sont exposées à des menaces de sécurité à grande échelle pour leurs informations et à des cyber-attaques destructrices, et ce quels que soient la taille, le secteur et la localisation des entreprises.

Si les systèmes de sécurité de l'information ne sont pas correctement gérés et mis à jour, les organisations courent le risque de subir de lourdes pertes financières et d'importantes atteintes à leur réputation.

Vérifier que votre organisation a mis en place les contrôles adéquats pour réduire les risques sérieux pour les données et éviter que les failles du système ne soient exploitées n'est plus une simple option.

Ces précautions sont encore plus incontournables depuis la publication du Règlement général sur la protection des données de l'UE, qui impose des exigences plus strictes et des amendes et sanctions plus lourdes aux organisations en cas de violation de données.

Notre expertise

La société LRQA est pionnière en matière d'élaboration de normes et s'est très tôt engagée dans les domaines de la certification et de l'évaluation des systèmes de management de la sécurité de l'information (SMSI).

De nombreux clients prestigieux dans des secteurs aussi divers que la finance, les télécommunications, l'édition de logiciels, la navigation sur Internet, le conseil, la justice et l'administration font confiance à LRQA pour leur fournir des évaluations de grande qualité, cohérentes et impartiales, assorties de services exhaustifs d'assistance spécialisée.

Nos évaluateurs regroupent des experts en systèmes de management, spécialisés en sécurité de l'information et dans d'autres aspects de l'informatique, dont la vision objective renforcera votre confiance dans vos propres mesures de sécurité estimées à l'aune des meilleures pratiques en vigueur dans le secteur.

À propos de LRQA

LRQA est une société reconnue comme étant le leader mondial des services de certification professionnelle. Nous sommes spécialisés dans la conformité des systèmes de management, ainsi que dans les avis d'experts pour un large éventail de normes, référentiels et services d'amélioration opérationnelle, incluant des programmes de formation et d'assurance sur mesure.

Nous sommes reconnus par près de 50 organismes d'accréditation et nos clients sont répartis dans plus de 120 pays.

Notre méthodologie d'évaluation unique permet de faire passer vos systèmes de management de la conformité à la performance. Ainsi, nous réduisons le risque pour votre entreprise tout en favorisant l'efficacité, l'efficience et l'amélioration continue de vos systèmes de management.

La méthodologie d'évaluation unique de LRQA vous aide à gérer vos systèmes et vos risques afin d'améliorer et de protéger les performances actuelles et futures de votre entreprise.

Lloyd's Register LRQA

Améliorer la performance, réduire le risque

Nos services d'évaluation et de formation en matière de sécurité de l'information

Nous proposons une gamme de services d'évaluation en ligne et en face à face adaptés aux organisations, quelles que soient leur taille et leur localisation, et nous pouvons vous aider à tirer le meilleur parti des normes.

Formation

Les packs et services de formation sur mesure de LRQA peuvent aider les organisations à n'importe quelle étape de leur SMSI.

Notre gamme de cours de formation inclut notamment les cours suivants :

- **Présentation de la norme ISO 27001:2013**
- **Mise en œuvre de la norme ISO 27001:2013**
- **Auditeur interne et auditeur en chef ISO 27001:2013**

Certification

Généralement, ce processus comprend deux étapes, une appréciation du système et une évaluation initiale, dont la durée dépend de la taille et de la nature de votre entreprise.

Votre responsable du développement des activités concevra une solution capable de répondre à vos besoins spécifiques tandis que nos évaluateurs, ouverts à toutes les options, vous assisteront et adopteront une approche pratique. Il s'agit là d'une des nombreuses manières d'enrichir réellement le processus d'évaluation.

Gap Analysis

Nos audits nous offrent l'occasion de faire ressortir les zones de faiblesse ou à risque de votre organisation afin de mettre au point un système certifiable. Elle peut également examiner les systèmes ou les processus de management existants et leur utilisation au sein de la norme sélectionnée.

Que l'installation de votre système de management n'en soit qu'à ses débuts ou que vous procédiez à une « répétition » avant l'évaluation proprement dite, vous pouvez décider du périmètre de « l'analyse des écarts » en accord avec votre responsable du développement ou avec l'évaluateur seul, de façon à bénéficier d'une plus grande souplesse au moment de déterminer le champ d'application et la durée du processus.

Surveillance

Une fois votre SMSI approuvé, nous effectuons régulièrement des visites de surveillance afin de vérifier l'efficacité de la solution. Vous avez ainsi l'assurance, ainsi que vos dirigeants, que les systèmes de management restent opérationnels et continuent de s'améliorer.

Évaluation du système de management intégrée

Les entreprises désireuses de combiner leur système de management avec un système existant (gestion de la qualité, par exemple) peuvent profiter d'un programme coordonné d'évaluation et de surveillance. Ce service est en constant développement.

Pour découvrir comment LRQA peut vous aider dans le cadre de la conformité aux exigences, rendez-vous sur **www.lrqa.fr**, envoyez un message à l'adresse **lrqa-lyon@lrqa.com** ou appelez le **04 72 13 31 41**.

Suivez-nous sur les réseaux sociaux :

www.lrqa.com